



Nortel Business Communications Manager 450 1.0

Administration and Security

Release 1.0

Document Revision 01.02

NN40160-601

Document status: Standard
Document issue: 01.02
Document date: July 2009
Product release: BCM450 1.0
Job function: Administration and Security
Type: Technical Publication
Language type: EN

Copyright © 2008-2009 Nortel Networks.
All Rights Reserved.

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.

Contents

New in this release	11
Features 11	
Business Element Manager 11	
Command Line Interface 11	
User accounts 11	
System-wide security policies 12	
Back up and restore operations 12	
Log management 12	
Software updates 12	
Diagnostic tools 12	
Introduction	13
Security fundamentals	15
System security considerations 15	
Secure protocols and encryption 17	
Security audits 17	
Site authentication 17	
Security certificate 18	
BCM450 SSL certificate properties 18	
Security policies 18	
User account and group management 23	
User account and group management navigation 23	
User accounts 23	
Default passwords 24	
Default user account groups 25	
Default access privilege (non-set) 29	
Telset access security 37	
Telset group access privileges 38	
User account blocking 39	
Accounts and Privileges 40	
Accounts and Privileges navigation 40	
Current account 40	
View by accounts 41	

- View by account: general 43
- View by account: remote access 44
- View by account: history 45
- View by account: group membership 46
- View by groups 46
- View by groups: general 47
- View by groups: members 47

Administration fundamentals

49

- Data backup and restore 49
 - Data backup and restore navigation 49
 - Scope of data backup and restore 49
 - Backup options 50
 - BCM450 backup file characteristics 51
 - Backup destinations 51
 - Restore optional components 53
 - Impact on system resources 53
 - Restore operations and logs 54
- Log management 54
 - Log management navigation 54
 - Overview of BCM450 logs 54
 - Log types 55
 - Log type navigation 55
 - Transferring and extracting logs 57
 - Log Browser 58
 - Log Browser navigation 59
- Hardware inventory 62
- Software updates and software inventory 62
- BCM450 utilities 63
 - Ping 63
 - Trace Route 63
 - Ethernet Activity 64
 - Reset 64
 - Diagnostic Settings 65
 - IP Set Port Details 65
- BCM Monitor 66
 - BCM Monitor—BCM Info tab 67
 - BCM Monitor—Media Card tab 68
 - BCM Monitor—Voice Ports tab 68
 - BCM Monitor—IP Devices tab 68
 - BCM Monitor—RTP Sessions tab 69
 - BCM Monitor—UIP tab 70
 - BCM Monitor—Line Monitor tab 70
 - BCM Monitor—Usage Indicators tab 71

System-wide security policies configuration **73**

- BCM450 system entry policy definition 73
 - Configuring system access control policy 73
- BCM450 local authentication policy definition 74
 - Configuring credential complexity 74
 - Configuring lockout on failed login policy 75
 - Configuring the idle session timeout 75
 - Configuring password expiry policy 76
 - Configuring password history policy 76
- BCM450 authentication service policy definition 77
 - BCM450 authentication service policy definition procedures navigation 77
 - Configuring the authentication method 77
 - Configuring the authentication server 78
 - Vendor specific attributes 79
- BCM450 SSL and SSH policy usage 81
 - BCM450 SSL and SSH policy usage procedures navigation 81
 - Uploading a Web Server Certificate 82
 - Transferring an SSH Key-Pair 82

Accounts, groups, and privileges configuration **85**

- BCM450 user account management 85
 - BCM450 user account management procedures navigation 85
 - Adding a new user account 85
 - Modifying a user account 86
 - Adding Telset access for a user 87
 - Deleting a user account 87
- BCM450 feature additions for dial-up users 88
 - BCM450 feature additions for dial-up users procedures navigation 88
 - Adding callback for a dial-up user 88
 - Adding NAT rules for a dial-up user 88
- BCM450 user password management 90
 - BCM450 user password management procedures 90
 - Changing a user password 90
 - Changing the current user password 91
- BCM450 user group management 91
 - BCM450 user group management procedures navigation 91
 - Creating a group 92
 - Deleting a group 92
 - Modifying group privileges 92
 - Adding a user account to a group 93
 - Deleting a user account from a group 93
- BCM450 account enabling and disabling 94
 - BCM450 account enabling and disabling procedures navigation 94
 - Reenabling a locked-out user 94

Enabling and disabling an account 95

Data backup and restore 97

On-demand backups 97

On-demand backup procedures navigation 97

Performing an immediate backup to your BCM450 97

Performing an immediate backup to your personal computer 98

Performing an immediate backup to a network folder 99

Performing an immediate backup to a USB storage device 100

Performing an immediate backup to an FTP server 100

Performing an immediate backup to an SFTP server 101

Scheduled backups 102

Scheduled backup procedures navigation 102

Accessing the schedule of regular backups 102

Modifying scheduled backups 102

Deleting scheduled backups 103

Creating a scheduled backup to BCM 104

Creating a scheduled backup to a network folder 105

Creating a scheduled backup to a USB storage device 107

Creating a scheduled backup to an FTP server 108

Creating a scheduled backup to SFTP server 109

Data restoration 111

Data restoration procedures navigation 111

Restoring a backup from BCM 111

Restoring a backup from a PC 112

Restoring a backup from a network folder 113

Restoring a backup from USB storage 114

Restoring a backup from an FTP server 115

Restoring a backup from an SFTP server 116

Restoring the factory default configuration 117

BCM450 log management system 119

Performing immediate log transfers 119

Performing an immediate log transfer to a USB storage device 119

Performing an immediate log transfer to a personal computer 120

Performing an immediate log transfer to a network folder 121

Performing an immediate log transfer to an FTP server 122

Performing an immediate log transfer to an SFTP server 123

Configuring scheduled log transfers 124

Creating a scheduled log transfer 124

Modifying a scheduled log transfer 126

Deleting a scheduled log transfer 127

Transferring log files using the BCM450 Web Page 128

Using the BCM450 Web Page to transfer logs to your personal computer 128

Using the BCM450 Web Page to transfer logs to other destinations 129

-
- Using the Log Browser 130
 - Extracting the log file 131
 - Specifying retrieval criteria 131
 - Filtering retrieval results 132
 - Viewing details for a single log record 133
 - Viewing details for multiple log records 133
 - Viewing log files using other applications 133

BCM450 hardware inventory 135

- Viewing and updating information about the BCM450 system 135
 - Viewing and updating information about the main unit 135
 - Viewing expansion daughter card information 136
 - Viewing and updating information about media bay modules 137
 - Viewing information about hard disk drives 138
 - Viewing and updating system expansion information 139
 - Viewing and updating information about digital mobility controllers 140
 - Viewing and updating other system information 141
- Viewing information about devices 142
 - Viewing information about attached devices 142
- Viewing additional information 143
 - Viewing additional information 143

BCM450 software updates 145

- Viewing the software update history 145
- Obtaining BCM450 software update 146
- Checking the status of a software update 147
- Applying a software update 147
 - Applying a software update from your personal computer 148
 - Applying a software update from a USB storage device 149
 - Applying a software update from a network folder 151
 - Applying a software update from an FTP server 152
 - Applying a software update from an HTTP server 154
- Scheduling a software update 155
- Modifying a scheduled software update 158
- Deleting a scheduled software update 159
- Viewing the software inventory 160
- Removing a software update 160

BCM450 utilities 163

- Pinging a device 163
- Tracing a route 164
- Viewing Ethernet activity 164
- Resetting and rebooting 165
 - Warm reset 165
 - Cold reset 165

Rebooting	166
Creating a scheduled reboot	167
Modifying a scheduled reboot	168
Deleting a scheduled reboot	169
Setting release reasons	169
Command Line Interface	170
Configuration CLI	170
Maintenance CLI	171
BCM Monitor installation and removal	173
Installing BCM Monitor (outside Element Manager)	173
Removing BCM Monitor (outside Element Manager)	174
BCM Monitor connection	175
Starting BCM Monitor within Element Manager	177
Starting BCM Monitor outside Element Manager	177
Disconnecting from a BCM system	178
Connecting to another BCM system	178
Using BCM Monitor	181
System status snapshots	181
Configuring BCM Monitor for static snapshots	182
Saving a static snapshot	184
Configuring BCM Monitor for dynamic snapshots	184
Using the dynamic snapshot utility	186
UIP information analysis	186
Enabling UIP message monitoring	187
Disabling UIP message monitoring	188
Logging UIP data	189
Accessing UIP log files	189
Disabling UIP timeout settings	189
Accessing message detail information elements	190
Clearing message detail information elements	190
Line summary	191
BCM Monitor statistics	191
Viewing current, minimum, and maximum values	191
Resetting logged minimum and maximum values	192
BCM450 service management system	193
Managing services	195
Viewing details about services	195
Stopping a service	195
Restarting a service	196
BCM450 Management Information Bases	197
Accessing MIB files	197

Accessing MIB files from the BCM450 web page	197
Accessing MIB files from the Nortel Customer Service site	197

New in this release

This is the initial release of the BCM450 platform. This document contains information about the tools available for administering and managing the BCM450 system in Release 1.0.

Navigation

- [Features \(page 11\)](#)

Features

This document contains information about the following features in Release 1.0.

Business Element Manager

Business Element Manager is the primary management application for BCM450 systems. The BCM Element Manager is a client-based management application that runs on a Windows computer or on a Citrix server. The Element Manager allows for connection to BCM450 devices over an IP network. It encompasses not only telephony programming, but also administrative functions such as backup management, software update management, and log management.

Command Line Interface

You can use the Command Line Interface (CLI) to configure basic settings, as well as shut down, reboot, or reset the BCM450 system. The CLI is available when you connect to the BCM450 through SSH using TCP/IP, or by connecting through a serial console. Two CLI modes are available: Maintenance CLI, and Configuration CLI. For more information about the diagnostic tools available, see [BCM450 utilities \(page 163\)](#) and [Using BCM Monitor \(page 181\)](#).

User accounts

The BCM450 supports a large number of user accounts. You can configure up to a total of 1999 user accounts, including the default accounts, such as nnadmin and nnguest. For more information about user accounts, see [Security fundamentals \(page 15\)](#) and [Accounts, groups, and privileges configuration \(page 85\)](#).

System-wide security policies

You can use Element Manager to configure system-wide security policies, such as authentication methods, password policies, and other access policies. For more information about security policies, see [Security fundamentals \(page 15\)](#) and [System-wide security policies configuration \(page 73\)](#).

Back up and restore operations

You can schedule back p operations, or perform on-demand backups to different storage locations. You can also use Element Manager to perform restore operations. For more information about backup and restore operations, see [Data backup and restore \(page 97\)](#).

Log management

You can view and manage log archives generated by the BCM450. For more information about managing logs, see [BCM450 log management system \(page 119\)](#).

Software updates

You can use Element Manger to apply software updates to the BCM450. You can also view an inventory of the software components installed on your system. For more information about software updates, see [BCM450 software updates \(page 145\)](#).

Diagnostic tools

The BCM450 provides a variety of diagnostic tools, including BCM Monitor, ping and route trace functions, and the ability to view Ethernet activity. For more information about the diagnostic tools available, see [BCM450 utilities \(page 163\)](#) and [Using BCM Monitor \(page 181\)](#).

Introduction

This document contains concepts, operations, and tasks related to the management features of the BCM450 system. This guide also describes additional administrative tasks, such as backups, software updates, monitoring, and inventory management.

Navigation

- [Security fundamentals \(page 15\)](#)
- [Administration fundamentals \(page 49\)](#)
- [System-wide security policies configuration \(page 73\)](#)
- [Accounts, groups, and privileges configuration \(page 85\)](#)
- [Data backup and restore \(page 97\)](#)
- [BCM450 log management system \(page 119\)](#)
- [BCM450 hardware inventory \(page 135\)](#)
- [BCM450 software updates \(page 145\)](#)
- [BCM450 utilities \(page 163\)](#)
- [BCM Monitor installation and removal \(page 173\)](#)
- [BCM Monitor connection \(page 175\)](#)
- [Using BCM Monitor \(page 181\)](#)
- [BCM450 service management system \(page 193\)](#)
- [BCM450 Management Information Bases \(page 197\)](#)

Security fundamentals

This chapter provides an overview of the BCM450 security policies, and outlines considerations that network administrators must take into account when they configure security policies.

The Security Policies panel allows you to establish system-wide security policies. This chapter describes the security policies that you can configure through the Element Manager.

Navigation

- [System security considerations \(page 15\)](#)
- [Secure protocols and encryption \(page 17\)](#)
- [Security audits \(page 17\)](#)
- [Site authentication \(page 17\)](#)
- [Security certificate \(page 18\)](#)
- [User account and group management \(page 23\)](#)
- [Accounts and Privileges \(page 40\)](#)

System security considerations

To define security parameters for users and the system, you must consider the level of security required to meet your network security standard. Note that the default security settings are not assigned to their maximum secure settings and you can change them to suit your specific requirements. If you change the default settings, ensure that you understand the interoperability implications between your system and client applications, the computer you use to access the system, and network impacts. For instance, some levels of security are not compatible with clients running Windows 95, 98, or ME.

Attention: Nortel recommends that you change all default system passwords after you verify system operation.

Consider the following questions when you design the security parameters for your system:

- Do you want administrative users to access the system through the Telset configuration menus?
- How much access to the Element Manager interface should you allow users?

Access is based on user privileges defined through user group membership. One default Element Manager administrator account (nnadmin) exists. This account includes a default Telset user ID and password. A read-only guest default account (nnguest) exists, which does not have a default Telset user ID and password. You can delete the guest account to increase security.

- Do you require a temporary account that expires?
- If the Element Manager receives no input from the user, how long do you want it to remain open?
- How long do you want a user account to remain locked out after a user enters specified number of incorrect passwords?
- How complex do you want user IDs and passwords in terms of length and character requirements?
- Do you want to use secure web access to Element Manager through Secure Sockets Layer (SSL). SSL encryption does not secure the Configuration Menu.
- Do you want modem access to use callbacks?
- Do you require the added security of a private SSL certificate?

Attention: Restrict core system configuration, such as resources and network management to an administrator-level account. Use the group profiles to define levels of users with access to the headings specific to their task. This also helps to prevent overlap programming if more than one person uses the interface at the same time.

Restrict the Dial-in access user group to users who require this interface. If users do not require modem access, disable the modem interface to provide further security.

Secure protocols and encryption

The BCM450 uses the following network protocols for Operation, Administration, and Maintenance (OAM) in a secured mode:

- CIM/XML is the main management protocol used by the BCM450 and is only available through an authenticated and authorized SSL connection. You can control user access based on assigned privilege levels.
- Multiple data transfer protocols are supported for the various applications including, SCP, SAMBA, and FTP.
- SSH is used by customer support personnel for troubleshooting purposes only. There are special authentication parameters for this interface.

Security audits

The system creates a security log file at system startup to record user logins and transactions. This log accumulates each day until it reaches the maximum log size, and the system deletes the oldest record to make room for the newest record. For information about managing logs, see [Data backup and restore \(page 97\)](#).

Administrators can view security logs using Log Management capabilities found on the Administration tab in Element Manager.

Each security log record contains

- the time of the event
- the user ID
- a summary of the action performed in the configchange.systemlog

Site authentication

The generic SSL certificate does not provide site authentication; a recognized signing authority does not sign the generic SSL certificate.

You can upgrade the SSL certificate used by the http server to a private SSL certificate, which offers site certification and encryption. Site authentication requires system-specific information, for example, an IP address, or a company name. A site-specific certificate ensures that when users point their web browser at the SSL web interface, the system does not ask users to accept the certificate.

If you use the default BCM450 generic SSL certificate, the system prompts the user to accept an unsigned certificate.

Security certificate

The BCM450 includes a generic SSL security certificate. The self-signed certificate enables SSL encryption functionality, and provides the necessary encryption keys.

A facility also exists to generate SSH certificates, required in the set up of an SSH server if you use Secure Copy (SCP) as a transfer method.

BCM450 SSL certificate properties

When you first log on to the Element Manager, a security alert appears that indicates site validation of the default certificate.

This security alert does not appear if you

- add a site-specific certificate
- suppress the message on your client browser

If you want a site-specific certificate, obtain a site certificate for your system from a Certificate Authority (CA) vendor. Certificate files must use the .PEM format. When you obtain a certificate and private security key, install them on the BCM450.

Attention: Ensure that you maintain a copy of your certificate and private security keys in a secure place, preferably offsite. This provides you with a backup if your system requires data reentry.

Security policies

You can use the BCM450 Security Policies pane in Element Manager to establish security policies that apply to the entire system, rather than to individual users.

The following table describes the fields in the Security policies pane:

Table 1 Security Policies field

Attribute	Value	Description
Entry Policy tab		
Disable Telset login	Check box	When selected, specifies when users cannot access the system through a Telset interface. Default: clear If the check box is selected, and DHCP changes the system IP address, you can determine the new IP address through the OAM port.
Disable post-login message	Check box	When selected, specifies that the post-login security warning does not open during log on. Default: clear

Table 1 Security Policies field

Attribute	Value	Description
Post-login message	Text	Displays the post-login security warning. You can edit the warning to customize the message for your system.
Nortel Support		
Hide Challenge Key	check box	When selected, displays asterisks to hide the characters used in the challenge key. Default: cleared.
Challenge Key	Text	<p>Specifies an alphanumeric key. The service technician requires this key as part of the access information to remotely access your system. Default: trust no one.</p> <p>If you change the default string, retain a record of the new string so that Nortel Technical Support can access your system during a support service call.</p> <p>Ensure the key is at least one character long to allow Nortel support operation.</p>
Local Authentication Policy tab		
Credential Complexity		
Credential Type	Element Manager: Alphanumeric Telset: Numeric	<p>Specifies the variety of characters an alphanumeric password must include. The complexity level defines the required number of each type of character</p> <p>User IDs are not case-sensitive).</p> <p>You must use a numerical Telset interface password. Password complexity for these passwords defines how many unique digits the system requires.</p>
Minimum User ID Length	Element Manager: Alphanumeric 1—32 Telset: Numeric 1—16	Specifies the minimum number of characters that the system requires for each type of credential.
Minimum password length	Element Manager: Alphanumeric 1—32 Telset: Numeric 1—16	<p>Specifies the minimum number of characters that you must enter for a new password.</p> <p>Alphanumeric passwords are case-sensitive.</p> <p>Ensure this setting is the same as or greater than the complexity level setting.</p> <p>For example, if you have a complexity level of two, two different types of characters or two unique numbers, ensure the password is at least two characters long.</p>

Table 1 Security Policies field

Attribute	Value	Description
Password complexity level (Element Manager)	0	Defines the number of character types that Element Manger requires for an alphanumeric password.
	1	
	2	0: No complexity checks
	3	1: one character type
	4	2: at least two character types
		3: at least three character types (default)
		4: all four character types
		A password complexity higher than 0 ensures that users cannot use a username as the password. Check minimum length setting to ensure that it is equal to or greater than the complexity level.
		Password complexity consists of the following types:
		upper case alphabet (English)
		lower case alphabet (English)
		westernized Arabic numbers
		non-alphanumeric characters (\$, !, %, ^, period, comma)
Password Complexity Level (Telset interface)	0	Specifies the number of unique digits that Telset requires as part of a password:
	1	
	2	0: No complexity checks
	3	1: one unique digit
	4	2: two unique digits
	5	3: three unique digits
		4: four unique digits
		5: prevent consecutive numbering
		A password complexity higher than 0 ensures that users cannot use a username as the password. Check the minimum length setting to ensure that it is equal to or greater than the complexity level.
Lockout on Failed Logon		
Enable lockout	check box	When selected, specifies that enable lockout rules apply to users.
Lockout counter	numeric value	Specifies the number of times the user can attempt to enter an invalid password before they become locked out. Default: 25; for increased security, change this number to 5.

Table 1 Security Policies field

Attribute	Value	Description
Lockout duration (min)	minutes	Specifies the amount of time after the user becomes locked out before they can log on again. Reset the lockout counter to zero. Default: 30.
Lockout counter reset	minutes	<p>Specifies the number of minutes after a lockout before the lockout counter automatically resets to zero. Default: 30.</p> <p>For example, if the lockout counter reset has a value of 30 minutes and a user enters invalid passwords, but does not reach the lockout counter threshold, and then waits 30 minutes before trying again, the lockout counter resets and begins counting from 1 again.</p> <p>If the user enters invalid passwords until they reach the lockout counter threshold, the Lockout duration determines when the user can log back on to the system.</p>
Password Expiry		
Enable password expiry	check box	When selected, specifies that the account expires at a specified time.
Days before password expire	up to 256	Enter the number of days the password can remain valid before it must be changed.
Warning days before password expire	numeric value	Enter the number of days prior to password expiry that a user receives notification.
Password History		
Enable password history	check box	When selected, the BCM stores a list of previously used passwords and prevents users from reusing them.
Password history length	numeric value	Enter the number of previously used passwords to store and check for this account, to prevent password reuse.
Authentication Service Policy tab		
Account management	menu	Specifies the method used to use to authenticate users when they log on. Options include Local Authentication and RADIUS. If you select RADIUS, you must also select the Enabled check box in the Radius Servers pane.
Server priority	Primary Secondary	Specifies which RADIUS server to use as the primary server for authentication, and which server to use as a secondary server to authenticate users when the primary server becomes unavailable.
Server name	alphanumeric	Name of the RADIUS server.
Server IP address	<IP address>	IP address of the RADIUS server.
Server Port	numeric	Port number of the RADIUS server.

Table 1 Security Policies field

Attribute	Value	Description
Enabled	check box	When selected, specifies to use RADIUS authentication. You must also select this check box before the BCM uses RADIUS authentication.
Server message timeout	numeric	Length of time to wait for the server to respond to a request for authentication before timing out. Nortel recommends that use a setting of 2.
Server retries	numeric	Number of times to retry connecting with the primary server before using an alternate means of authenticating the user. Nortel recommends that you use a setting of 2.
Server shared secret	alphanumeric	Key required for the BCM to communicate with the RADIUS server. Nortel recommends that you use a key at least 64 characters in length.
Session Management Policy tab		
Session time out (min.)	minutes	Specifies the number of minutes a logged in user account can remain inactive before the system ends the session and logs out the account. If you leave this field blank, the session is ends only when the user logs off.
Active sessions		
User ID	Read-only	Displays the user ID of the active session.
IP address	Read-only	Displays the IP address of the active session.
Login date	Read-only	Displays the log on date of the active session.
SSL and SSH Policy tab		
SSL		
Install Web Server Certificate (SSL)	Button	Downloads application security certificates to the server where SSH runs to ensure a secure copy connection for operations, such as backup and restore, upgrades and patches.
SSH		
Fingerprint	alphanumeric	Displays an identifier for the application security certificate.
Generate new SSH key-pair	Button	Opens the file system browser to allow a system-specific security certificate and the accompanying Private key to be selected for SSL.
Transfer Public Key	Button	Downloads a public security certificate.

User account and group management

This section contains information on how to manage user accounts and groups

User account and group management navigation

- [User accounts \(page 23\)](#)
- [Default passwords \(page 24\)](#)
- [Default user account groups \(page 25\)](#)
- [Default access privilege \(non-set\) \(page 29\)](#)
- [Telset access security \(page 37\)](#)
- [User account blocking \(page 39\)](#)

User accounts

User accounts are defined by

- a unique user ID visible only to authenticating services; Element Manager IDs are alphanumeric and Telset IDs are numeric.
- a unique user name assigned for either or both the Element Manager and Telset configuration that includes a minimum length that you define when you configure the security policies.
- a unique password assigned for any defined user ID. Passwords must satisfy the Password Policy settings for the system that you define when you configure the security policies.
- a list of group attributes that allow the user specific access privileges in the system

After you create an account, you can assign groups to that account. Groups are sets of privileges based on user tasks or roles. For example, if you have a user who is responsible for remote monitoring, you can create an account for that user and then assign a group to the account; the group that you assign would contain the appropriate privileges for that role. The BCM has default groups available, but you can refine the privileges available within a group to suit the needs of your network. In this example, you could assign the default group called Remote Monitoring, which would allow the user to do such things as view metrics and alarms.

The User ID of the account profiles created through the set based interface cannot be modified through the Element Manager.

Two default user accounts are provided:

- The nnadmin account is read only and cannot be deleted or disabled

- The nnguest account provides customers with web-only access. All access to the Apache web server requires a valid administrator username and password

Auditing for user accounts includes:

- creation date, time, and the user ID that created the account
- modify date, time, and the user ID that modified the account
- expiry date and time, if enabled
- login history, including failed attempts and the date and time of the last successful attempt
- an audit log that tracks logged-in user transactions, including user account changes

Remote users can have a callback number assigned as well. This feature allows authentication of remote users calling in through a modem. After authentication, the BCM450 will call the user back at the number specified.

Nortel recommends that each user have a separate user account (User Name) with a unique password. These are set up by a user with administrator privileges in the Element Manager. The password only shows up as asterisks on the Element Manager panel. If the password is lost, the administrator can reset the password for the user by re-entering the password in the user account. Each user can access their own user information and change their password. User accounts can be disabled, either manually or through dated expiry.

On the Telset administration menu (F9*8), only the administrator (SBAInstaller) can enable or disable the Telset user IDs and modify or delete Telset user passwords.

Default passwords

The following table lists the available default passwords for the Element Manager interface, the Telset interface, and the voice mail interface.

Table 2 Default passwords

User ID	Default passwords	Telset ID	Default Telset password	Function	Available at startup?
nnadmin	PlsChgMe!	738662	266344	Read-only installer/system administrator	Yes
nnguest	nnguest			Read-only web-only access	Yes
		738266	266344	Set-based installer level	No
		738727	727587	Set-based administration	No

Table 2 Default passwords

User ID	Default passwords	Telset ID	Default Telset password	Function	Available at startup?
		738236	23646	Set-based coordinator functions	No
		738227	22742	Set-based basic access	No
voicemail admin	PlsChgMe!	738862	266344	Voice mail administration (see Note 1)	No
Note 1: This account is not created by default. You must add a voice mail account using F9*8.					

New accounts are created from the startup profile with a default password of Time4Chg!

Attention: The default Administrator password includes full access to the system. Change the default password as soon as the initial system setup completes and system function is verified.

Default user account groups

The BCM450 includes a number of default read-only groups that provide a predetermined set of access privileges. You can assign additional privileges to groups. The following table lists the default privilege levels for each default group, described in [Default access privilege \(non-set\) \(page 29\)](#) and [Telset access security \(page 37\)](#).

Table 3 Default user account groups

Group name	Privileges	Notes
SBA Installer	SBAInstaller IP Set Registration	SBA - Installer group access privileges (page 38) IP Set Registration access privileges (page 30)
SBA Coordinator+	SBASystemCoord	SBA - System Coordinator and group access privileges (page 38)
SBA Coordinator	SBASystemCoordBasic Guests	SBA - System Coordinator group access privileges (page 38) Guests access privileges (page 33)
SBA Basic	SBABasic	SBA - Basic group access privileges (page 39)
Voice Mail & Contact Center Group	VoiceMailAdmin	If the user account is only assigned this group, the user will only be able to access the voice mail and Contact Center administration. Voice Mail and Contact Center access privileges (page 29)

Table 3 Default user account groups (continued)

Contact Center	Contact Center	If the user account is only assigned this group, the user will only be able to access Contact Center administration. Contact Center access privileges (page 29)
CDR Application	CDRApp	If the user account is only assigned this group, the user will only be able to access Call Detail Recording (CDR) functions. CDR App access privileges (page 31)
CTE Application	CTEApp	CTE App access privileges (page 30)
BCM Monitor Application	Application - BCM Monitor	BCM Monitor Appl access privileges (page 31)
Administrator	SBA	IP Set Registration access privileges (page 30)
	IP Set Registration	
	Application - BCM Monitor	BCM Monitor Appl access privileges (page 31)
	CDRApp	CDR App access privileges (page 31)
	PPP Login	PPP Access access privileges (page 31)
	AdminDownload	Admin Download access privileges (page 32)
	Exclusive Access	Exclusive Access access privileges (page 32)
	Admin	Admin access privileges (page 32)
	DataAdmins	DATA Admins group access privileges (page 32)
	Remote Access	Remote Access access privileges (page 33)
	Voice Admins	Voice Admins access privileges (page 33)
	Software Upgrade	Software Upgrade access privileges (page 35)
	Alarm Viewer	Alarm Viewer access privileges (page 35)
	SBA Installer Security	SBA - Installer group access privileges (page 38)
	CTE Appl	CTE App access privileges (page 30)
	Operational Logs	Operational Logs access privileges (page 36)
	Diagnostic Logs	Diagnostic Logs access privileges (page 36)
	Modem dial out	Modem dial out access privileges (page 36)
	ISDN dial in	ISDN dial in access privileges (page 36)
	ISDN dial out	ISDN dial out access privileges (page 36)
Data Admin	DATAAdmins	DATA Admins group access privileges (page 32)

Table 3 Default user account groups (continued)

Remote Access	PPP RemoteAccess	Remote Access access privileges (page 33)
Guest	Guests	Guests access privileges (page 33)
Voice Admin	IP Set Registration VoiceMail Admins Alarm Viewer	IP Set Registration access privileges (page 30) Voice Admins access privileges (page 33) Alarm Viewer access privileges (page 35)
Power Users	SBA - IP Set Registration DATAAdmins VoiceMailAdmin Alarm Viewer	IP Set Registration access privileges (page 30) DATA Admins group access privileges (page 32) Voice Admins access privileges (page 33) Alarm Viewer access privileges (page 35)
Backup Operators	BackupOperators	Backup Operators access privileges (page 34)
Security	Security AdminDownload Diagnostic Logs Operational Logs	Security access privileges (page 29) Admin Download access privileges (page 32) Diagnostic Logs access privileges (page 36) Operational Logs access privileges (page 36)
Admin Download	AdminDownload	Admin Download access privileges (page 32)
Guest Download	GuestDownload	Can access the BCM450 Web page for application downloads and user documentation. Guests access privileges (page 33)
Remote Monitoring	Remote Monitor Operational Logs	Remote Monitoring access privileges (page 35) Operational Logs access privileges (page 36)
Software Upgrade	Software Upgrade	Software Upgrade access privileges (page 35)

Table 3 Default user account groups (continued)

Local Administrator	Admin	Admin access privileges (page 32)
	Admin Download	Admin Download access privileges (page 32)
	Alarm Viewer	Alarm Viewer access privileges (page 35)
	Application - BCM Monitor	BCM Monitor Appl access privileges (page 31)
	BackupOperators	Backup Operators access privileges (page 34)
	Business Applications	
	CDR Application	CDR App access privileges (page 31)
	CTE Application	CTE App access privileges (page 30)
	Contact Center	If the user account is only assigned this group, the user will only be able to access Contact Center administration. Contact Center access privileges (page 29)
	DATAAdmins	DATA Admins group access privileges (page 32)
	Diagnostic Logs	Diagnostic Logs access privileges (page 36)
	Exclusive Access	Exclusive Access access privileges (page 32)
	Guests	Guests access privileges (page 33)
	GuestDownload	Can access the BCM450 Web page for application downloads and user documentation. Guests access privileges (page 33)
	Operational Logs	Operational Logs access privileges (page 36)
	Remote Access	Remote Access access privileges (page 33)
	Remote Monitor	Remote Monitoring access privileges (page 35)
	SBA - IP Set Registration	IP Set Registration access privileges (page 30)
	SBABasic	SBA - Basic group access privileges (page 39)
	SBAInstaller	SBA - Installer group access privileges (page 38)
	SBASystemCoordBasic	SBA - System Coordinator group access privileges (page 38)
	Security	Security access privileges (page 29)
	Software Upgrade	Software Upgrade access privileges (page 35)
	System - Serial Port	
	Voice Admins	Voice Admins access privileges (page 33)
	VoiceMailAdmin	Voice Admins access privileges (page 33)

Default access privilege (non-set)

The group privileges further refine access availability to groups and users. You can assign more than one privilege to a group and more than one group to a user account. The group with the most privileges defines what the user can access.

For instance, the Admin includes has all privileges; therefore, if this group is assigned to the user, any other group assignments with less access are superseded.

The default privileges are arranged as profiles with access privileges. The sections below list access privileges for each profile.

Voice Mail and Contact Center access privileges

You can set access privileges for:

- SBA - Voice Mail
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - CONFIG - Applications - Voice Messaging
- EM - CONFIG - Applications - Contact Center
- Web Documentation - User Documentation
- BCM450 Applications - Applications - CallPilot Manager
- Web - User Applications

Contact Center access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - Applications - CallPilot Manager
- Web - User Applications

Security access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - CONFIG - Administrator Access - Accounts and Privileges

- EM - CONFIG - Administrator Access - Security Policies
- EM - CONFIG - Administrator Access - SNMP
- EM - CONFIG - Administrator Access - Dial In
- EM - CONFIG - Administrator Access - Dial Out
- EM - CONFIG - Telephony - Call Security
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - General - SNMP Trap Setting
- EM - ADMIN - General - Service Manager
- EM - ADMIN - Utilities - Reset
- EM - ADMIN - Software Management - Software Inventory Panel (read-only)
- Web Documentation - User Documentation
- Diagnostic Logs - Diagnostic Log Transfer - Diagnostic Only component logs
- SSL Certificate Transfer - Certificate Transfer - SSL Certificate and SSH Key upload or download
- Web - User Applications

CTE App access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - Applications - CTE DA Pro AE
- Web - User Applications

IP Set Registration access privileges

You can set access privileges for:

- SBA - IP Set Registration
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- Web - User Applications

BCM Monitor Appl access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- BCM450 Applications - Applications - BCM Monitor
- Web - User Applications

CDR App access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - Applications - Call Detail Recording
- Web - User Applications

PPP Access access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- RAS - Applications - PPP
- Web - User Applications

Guest Download access privileges

You can set access privileges for:

- Web Documentation - User Documentation
- Web Application Download - Web Download - Callpilot Unified Messaging
- Web Application Download - Web Download - Desktop Assistant
- Web Application Download - Web Download - Desktop Assistant Pro
- Web Application Download - Web Download - 2050 Soft Phone
- Web Application Download - Web Download - Personal Call Manager

- Web Application Download - Web Download - Lan CTE Client

Admin Download access privileges

You can set access privileges for:

- Web Documentation - User Documentation
- Web Documentation - Admin Documentation
- Web Application Download - Web Download - Element Manager
- Web Application Download - Web Download - NCM for BCM450
- Web Application Download - Web Download - Callpilot Unified Messaging
- Web Application Download - Web Download - Desktop Assistant
- Web Application Download - Web Download - Desktop Assistant Pro
- Web Application Download - Web Download - 2050 Soft Phone
- Web Application Download - Web Download - Personal Call Manager
- Web Application Download - Web Download - Lan CTE Client
- Web Application Download - Web Download - BCM Monitor
- Web Application Download - Web Download - CDR Client Wrapper Utility
- Web Application Download - Web Download - SSH

Exclusive Access access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- Web - User Applications

Admin access privileges

You can set all access privileges.

DATA Admins group access privileges

You can set access privileges for:

- EM - CONFIG - System - IP Subsystem
- EM - CONFIG - Administrator Access - Current User
- EM - CONFIG - Administrator Access - Dial In

- EM - CONFIG - Administrator Access - Dial Out
- EM - CONFIG - Resources - Media Gateways
- EM - CONFIG - Data Services- DHCP Server Settings
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - Utilities - BCM Monitor
- EM - ADMIN - Utilities - Ping
- EM - ADMIN - Utilities - Trace Route
- Web Documentation - User Documentation
- Web - User Applications

Remote Access access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - CONFIG - Administrator Access - SNMP
- EM - CONFIG - Administrator Access - Dial In
- EM - CONFIG - Administrator Access - Dial Out
- EM - ADMIN - General - SNMP Trap Destinations
- Web Documentation - User Documentation

Guests access privileges

You can set access privileges for:

- Read-only access to all but Utilities, Backup and Restore, and Log Management
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- Web - User Applications

Voice Admins access privileges

You can set access privileges for:

- EM - CONFIG - System - Identification
- EM - CONFIG - System - Time and Date

- EM - CONFIG - System - Keycodes
- EM - CONFIG - System - IP Subsystem
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - CONFIG - Resources - all
- EM - CONFIG - Telephony - all
- EM - CONFIG - Data Services - DHCP Server Setting
- EM - CONFIG - Applications - LAN CTE
- EM - CONFIG - Applications - Voice Messaging/Contact Center
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - General - Hardware Inventory
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - System Metrics - Qos Monitor
- EM - ADMIN - System Metrics - NTP Metrics
- EM - ADMIN - Telephone Metrics - all
- EM - ADMIN - Utilities - BCM Monitor
- EM - ADMIN - Utilities - Reset
- EM - ADMIN - Software Management - all as read only
- Web Documentation - User Documentation

Backup Operators access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - ADMIN - Backup and Restore - Backup
- EM - ADMIN - Backup and Restore - Restore
- Web Documentation - User Documentation
- Web - User Applications

Remote Monitoring access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - ADMIN - General - Alarm as read only
- EM - ADMIN - General - Alarm Setting as read only
- EM - ADMIN - General - SNMP Trap Destinations
- EM - ADMIN - General - Service Manager as read only
- EM - ADMIN - General - Hardware Inventory as read only
- EM - ADMIN - System Metrics - Qos Monitor
- EM - ADMIN - System Metrics - UPS Metrics as read only
- EM - ADMIN - System Metrics - NTP Metrics as read only
- EM - ADMIN - Telephone Metrics - all
- EM - ADMIN - Utilities - BCM Monitor
- Web Documentation - User Documentation
- Web - User Applications

Software Upgrade access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - ADMIN - Utilities - Reset
- EM - ADMIN - Software Management - all
- Web Documentation - User Documentation
- Web - User Applications

Alarm Viewer access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- EM - ADMIN - General - Alarm
- EM - ADMIN - General - Alarm Setting
- EM - ADMIN - General - Hardware Inventory

- Web Documentation - User Documentation
- Web - User Applications

Operational Logs access privileges

You can set access privileges for:

- Web Documentation - User Documentation
- EM - ADMIN - Logs - Management
- Web - User Applications

Diagnostic Logs access privileges

You can set access privileges for:

- Web Documentation - User Documentation
- EM - ADMIN - Logs - Management

Modem dial out access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out using analog modem

ISDN dial in access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out using ISDN

ISDN dial out access privileges

You can set access privileges for:

- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User

- Web Documentation - User Documentation
- Web - User Applications
- PPP dial out using ISDN

Telset access security

You can use the Telset administration interface (FEATURE 9*8) to activate or deactivate the Telset default access user accounts. You can also use this interface to change the password for these accounts. For further information about using Telset features, see the Telset Admin Guide.

The Telset group privileges apply specifically to the following Telset interfaces:

- FEATURE 9*8 (Administrator access only)
- FEATURE **266344 (**CONFIG) (telephony interface)
- FEATURE 983 (CallPilot interface)

Use the preceding interfaces only as supplementary configuration portals. You can also block access to these interfaces when you configure the system security policies.

Table 4 Default Telset group access privileges

User ID	Default password	Telset ID	Default Telset password	Function	Available at startup?
nnadmin	PlsChgMe!	738662	266344	Read-only installer/system administrator	Yes
nnguest	nnguest			Read-only web-only access	Yes
		738266	266344	Set-based installer level	No
		738727	727587	Set-based administration	No
		738236	23646	Set-based coordinator functions	No
		738227	22742	Set-based basic access	No
voicemailadmin	PlsChgMe!	738862	266344	Voice mail administration	No

Telset group access privileges

There are four set-based group access privileges. The following sections list the access privileges in order of greatest to least.

SBA - Installer group access privileges

You can set access privileges for:

- SBA - FEATURE 9*8
- SBA - Installer Rights
- IP Set Registration (when IP set registration is configured and a global password setting is used)
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - User Applications

SBA - System Coordinator and group access privileges

You can set access privileges for:

- SBA - Coordinator Plus Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - User Applications

SBA - System Coordinator group access privileges

You can set access privileges for:

- SBA - Coordinator Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - User Applications

SBA - Basic group access privileges

You can set access privileges for:

- SBA - Basic Rights
- EM - CONFIG - Administrator Access - Accounts and Privileges - Current User
- Web Documentation - User Documentation
- BCM450 Applications - User Applications

User account blocking

Different methods exist to block user access to the system based on your security and administrative requirements.

- You can block unauthorized access by ensuring that you change all default passwords after the system is set up and verified.
- You can also block user access by simply changing the password. Retain a record of the password, as this information does not appear either on the Element Manager pane or in the programming record file.
- You can increase the complexity required for both Element Manager and Telset passwords to make it difficult for unauthorized users to inadvertently guess the correct password. Increase complexity by increasing the type of characters required and the minimum length of the password.
- You can configure the system to lock out a user if they enter the password incorrectly a (configurable) number of times. You can unlock the account through the user account record, or the user can wait for the lockout timer to run out before attempting to log on again. The user account shows the last time a user failed to log on.
- You can configure a user account to automatically expire on a given date.
- You can manually disable the account. If the user is currently logged in, this takes effect at the next logon attempt.

If you want to decrease the amount of system access, you can delete groups and reassign groups with lower access privileges to the user account.

The administrator that performs maintenance tasks can lock the system during the duration of the maintenance. Any user already logged on remains logged on, but cannot log on again until the Exclusive Access timer runs out.

Accounts and Privileges

This section describes the tabs and fields available on the Accounts and Privileges pane.

Accounts and Privileges navigation

- [Current account \(page 40\)](#)
- [View by accounts \(page 41\)](#)
- [View by groups \(page 46\)](#)

Current account

The Current Account tab provides a summary of user information about the person currently signed into Element Manager.

Table 5 Current account tab

Attribute	Value	Description
Account Notifications	Read-only	This field displays account notifications, such as notifications of password expiries.
User ID	Read-only	A read-only field that a user with administrator privileges can change on the user accounts pane.
Password	Alphanumeric	Requires a password entry that contains all the security requirements. Changes to the password take effect at the next logon session.
Telset user ID	Read-only	A read-only field that a user with administrator privileges can change on the user accounts pane.
Telset password	Numeric	Requires a numeric password entry unique for each user. These strings must satisfy the security requirements. This password takes effect at the next logon session.
Last Successful login	Read-only	Indicates the last date and time the user account was used to log on to the system (read only).
Account Management	Read-only	Displays the method used to authenticate the user session: local authentication or centralized authentication through a RADIUS server.
Failed Login History		
Last failed login	read-only	Displays the date and time of the last failed login.
From		Displays the interface from which the login was attempted.
Failed Telset Login History		
Last failed login	read-only	Displays the date and time of the last failed login by a Telset user.

Table 5 Current account tab

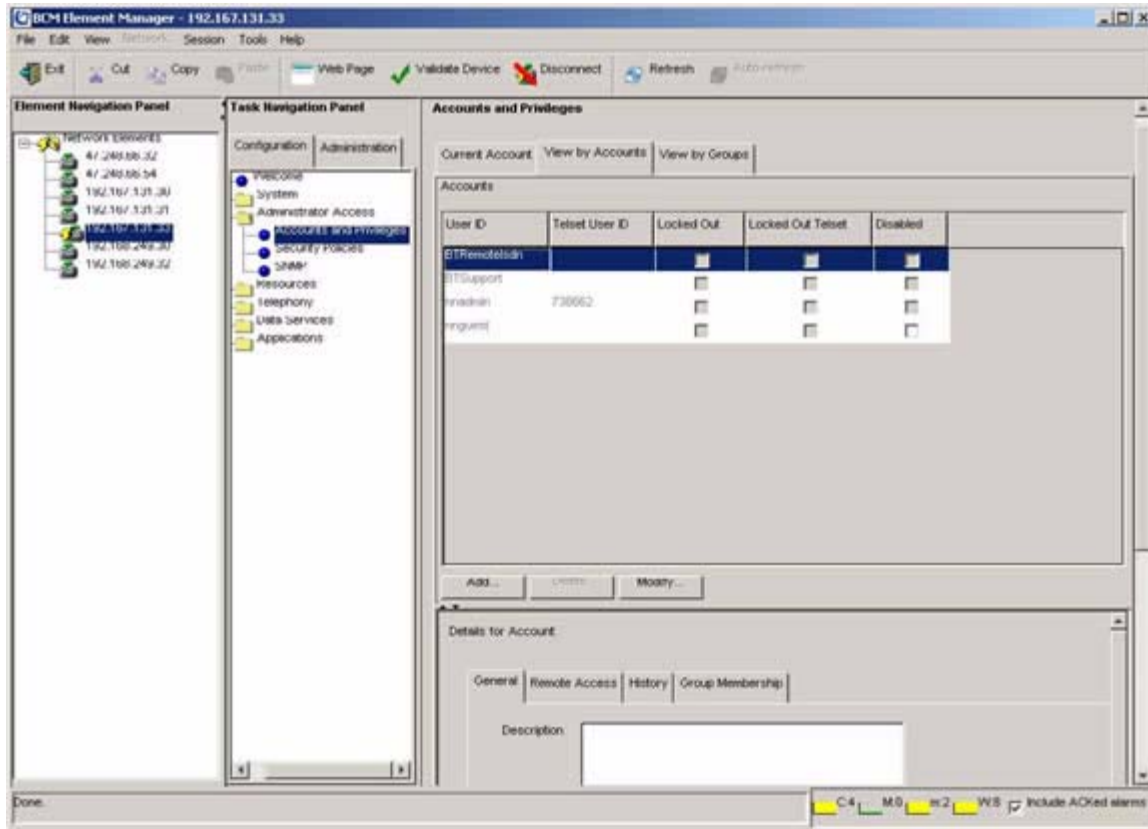
Attribute	Value	Description
From		Displays the interface from which the login was attempted.
Exclusive Access		
Exclusive access time remaining	numeric seconds	Specifies the amount of time left before other users can log on to the system. Visible only to users with administrator privileges.
Buttons		
Enable Exclusive Access	numeric minutes	Opens the Enable Exclusive Access dialog box from which you enter the amount of time that you want to have exclusive access to the system. Exclusive Access does not disable the access of users who are currently logged on. Visible only to users with exclusive access privileges.
Disable Exclusive Access		Stops the exclusive access timer and allows other users back on to the system. Visible only to users with exclusive access privileges.

View by accounts

The View by Accounts tab contains the table that defines individual user accounts. In this table you define how the system identifies the user. You also define what privileges the user has by assigning the user to groups.

You can add, delete, or modify user account information in the table. When you add or modify a user, you can enter a password for both the Element Manager interface and the Telset interface.

Figure 1 Accounts and Privileges, View by Accounts tab



The following table shows the fields of the View by Accounts tab.

Table 6 View by Accounts fields

Attribute	Value	Description
User ID	alphanumeric	Displays the accounts by User ID
Telset User ID	numeric	Displays the accounts by Telset User ID
Locked Out	Check box	Indicates if a user is locked out. When selected, the user cannot access the system. This field becomes selected when a user enters an incorrect password too many times, and the system locks the user account. The user must wait for the lockout timer to run out, or an administrator can unlock the user account using "Re-enable a locked-out user" on page 123 .
(1 of 2)		

Table 6 View by Accounts fields

Attribute	Value	Description
Locked Out Telset	Check box	Indicates if a user is locked out. When selected, the user cannot access the system. This field becomes selected when a user enters an incorrect password too many times, and the system locks the user account. The user must wait for the lockout timer to run out, or an administrator can unlock the user account using “Re-enable a locked-out user” on page 123 .
Disabled	Check box	Indicates if a user account is disabled. When selected, the user cannot access the system. This field becomes selected when the account expiry date is reached. See “Enabling and disabling an account” on page 124 .
Buttons		
Add		Opens the Add Account dialog box
Delete		Deletes the selected user account
Modify		Opens the Modify Account dialog box
(2 of 2)		

Attention: You cannot delete the nnadmin user; therefore, ensure that you change the default password as soon as possible after system setup. Keep a record of the password in a safe place.

If you select a user on the Users list, two additional panes appear in the lower frame:

- Use the General pane to see the current status of the account. See [View by account: general \(page 43\)](#)
- Use the Group Membership pane to associate the account to group profiles, which determines user access. See [View by account: group membership \(page 46\)](#).

View by account: general

The General panel provides user account information and account control settings.

The following table describes each field on this pane.

Table 7 View by Accounts: General fields

Attribute	Value	Description
Description	Alphanumeric	Displays the descriptive name and information for the user or the user function. You can leave this field blank.
Account Expiry		
Account will be disabled on	Date	Specifies the date and time when the user account expires. The menu opens a calendar.
Enable account expiry	Check box	When selected, specifies that the user account automatically expires at the specified date and time.
Account Textual Credentials		
Password expiry	Menu	Specifies the date to force a password change.
Change password on login	Check box	When selected, forces a user to change his or her password when logging on.
Account Telset Credentials		
Password expiry	Menu	Specifies the date to force a Telset password change.
Change password on login	Check box	When selected, forces a Telset user to change his or her password when logging on.

View by account: remote access

The Remote Access pane provides callback settings to verify user information, as well as configuration of NAT rules for dial-up users. The following table describes each field on this pane.

Table 8 View by Accounts: Remote Access

Attribute	Value	Description
Modem Callback Number	Telephone #	Specifies the number the system will call to verify the dial-up user access
Modem Callback Passcode	User ID	Specifies the passcode the system uses to confirm the callback is legitimate
ISDN Callback Number	Telephone #	Specifies the number the system will call to verify the ISDN user access
IP Address		
BCM IP Address	IP address	Specifies the PPP IP address of the BCM when connecting with analog modem or ISDN terminal adaptors.
NAT Rules*		
Rule 1: Dial-in Side	IP address	Enter an IP address on a dial-in interface to be translated.
LAN Side	IP address	Enter an IP address on the local LAN to use when translating the dial-in address in Rule 1.

Table 8 View by Accounts: Remote Access

Attribute	Value	Description
Rule 2: Dial-in Side	IP address	Enter an IP address on a dial-in interface to be translated.
LAN Side	IP address	Enter an IP address on the local LAN to use when translating the dial-in address in Rule 2.
Rule 3: Dial-in Side	IP address	Enter an IP address on a dial-in interface to be translated.
LAN Side	IP address	Enter an IP address on the local LAN to use when translating the dial-in address in Rule 3.
Rule 4: Dial-in Side	IP address	Enter an IP address on a dial-in interface to be translated.
LAN Side	IP address	Enter an IP address on the local LAN to use when translating the dial-in address in Rule 4.
Note 1: Multicast IP addresses cannot be used for NAT rules.		

View by account: history

The History pane provides user account and log on histories and account control settings.

The following table describes each field on this pane.

Table 9 View by Accounts: History fields

Attribute	Value	Description
Account history		
Account created	Read-only	Specifies the date that the user record was added.
Created by		Specifies the user ID of the person who added the user account.
Last Modified	Read-only	Specifies the date the user record was last modified.
Modified by		Specifies the user ID of the person who last modified the account.
Login history		
Last successful login	Read-only	Specifies the date the user last successfully logged on to the Element Manager.
Failed login count	Read-only	Specifies the number of times the user tried and failed to log on before successfully logging on or becoming locked out. If the count matches the failed login threshold, a value of true appears in the Locked Out column on the Accounts table.
Last failed login	Read-only	Specifies the date that the user last tried and failed to log on.
From	Read-only	Element Manager: Displays the IP address of the Element Manager
Telset login history		

Table 9 View by Accounts: History fields

Attribute	Value	Description
Last successful login	Read-only	Specifies the date the user last successfully logged on to Telset.
Failed login count	Read-only	Specifies the number of times the user tried and failed to log on before successfully logging on or becoming locked out. If the count matches the failed login threshold, a value of true appears in the Locked Out column on the Accounts table.
Last failed login	read-only	Specifies the date that the user last tried and failed to log on.
From	read-only	Telset: Displays the DN of the telephone used to log on to the system.

View by account: group membership

Use the Group Membership pane to associate the user account with one or more functional groups. The user gains all the privileges assigned to each group added to the list. The following table describes each field on this pane.

Table 10 Group membership fields

Attribute	Value	Description
Account is Member of Groups	Default groups	Lists groups the user belongs to. See Telset group access privileges (page 38) for a list of the default groups and the privileges associated with each. Add, modify and delete groups from the View by groups (page 46) pane.
Buttons		
Add		Opens the Add Account dialog box. Choose the group or groups with the appropriate access privileges for the user. You cannot add user accounts to groups with read-only privileges.
Delete		Deletes the user account from the selected group.

View by groups

Use the View by Groups pane to add or delete members from group profiles. The Groups pane lists all the groups currently available in the system. The following table describes each field on this pane.

Table 11 EM view by groups

Attribute	Description
Groups	Lists all the defined groups. See Telset group access privileges (page 38) for a list of the default groups and associated privileges.
Buttons	

Table 11 EM view by groups

Attribute	Description
Add	Opens the Add Group dialog box. Allows the creation of custom groups that provide combinations of privileges not covered by the default groups.
Delete	Opens the Confirm Delete dialog box. Allows for the deletion of any group, with the exception of the Admin Group.

For details about groups, See the panes described in [View by account: general \(page 43\)](#).

View by groups: general

For a selected entry in the Groups table, you can use the General details pane to define the system privileges assigned to this group, and to users assigned with this group. This pane also provides status information for the group. The following table describes each field on this pane.

Table 12 View by Groups: General panel fields

Attribute	Value	Description
Group History		
Group created	read-only	Specifies the date the group account was created
Created by		Specifies the user who created the account
Last modified	read-only	Specifies the last date the group account was changed
Modified by		Specifies the user who performed the changes
Group Privileges: Privileges		
Privilege	read-only	Lists the system access privileges allowed to members of the selected group
Actions:		
Add		Opens the Add Privilege to Group dialog box. Allows the privilege to be added to the group
Delete		Opens the Confirm Delete dialog box. Allows the privilege to be deleted from a group

View by groups: members

For a selected group in the Groups table, you can use the Members pane to assign the group to existing user accounts and to view which accounts have the selected group assigned.

The following table describes each field on this pane.

Table 13 View by Groups: Group Membership fields

Attribute	Value	Description
Description	Read-only	Lists the user accounts in the selected group.
User ID	Alphanumeric	Displays the accounts by user ID.
Telset User ID	Numeric	Displays the accounts by Telset user ID.
Buttons:		
Add		Opens the Add Account to Group dialog box. Allows the user account to be added to the selected group.
Delete		Deletes the selected user account from the selected group.

Administration fundamentals

This chapter provides an overview of administration fundamentals, such as backup and restore operations, system logs, and utilities.

Navigation

- [Data backup and restore \(page 49\)](#)
- [Log management \(page 54\)](#)
- [Hardware inventory \(page 62\)](#)
- [Software updates and software inventory \(page 62\)](#)
- [BCM450 utilities \(page 63\)](#)
- [BCM Monitor \(page 66\)](#)

Data backup and restore

This section provides information about how to back up and restore data from the BCM450 system.

Data backup and restore navigation

- [Scope of data backup and restore \(page 49\)](#)
- [Backup options \(page 50\)](#)
- [Restore optional components \(page 53\)](#)

Scope of data backup and restore

Before you make administrative changes or as your BCM450 system accumulates information, you can create a backup archive on the BCM itself, on a USB drive, or in another location on the network. At a later time, you can restore the data to the BCM450.

Attention: Nortel recommends that you back up BCM450 data on a regular basis. In particular, you should perform a backup of the BCM450 data before you undertake major configuration changes and before you apply a software update or upgrade.

You can restore data to the same system or to a different system at the same software release level. The BCM450 checks the software release level of the destination system and provides a warning if an incompatibility prevents the backup from restoring onto the selected system.

You can also restore data to a system that you upgraded to the next hardware release level. For example, you can create a backup archive of a system, upgrade that system to the next hardware release level, and then restore the programming and configuration settings. On BCM450 systems equipped with a BRI module, you need to reconfigure the telephony resources and trunks associated with the module after you perform a restore operation.

All passwords and database records included with your backup file are encrypted. When you perform a restore operation, the password on the target system must match the password used when you created the backup archive.

You can perform backup operations on demand or you can schedule a single backup or recurring backups. You can view the backup schedule and change it as required, and you can also save a record of the backup schedule that you configured.

You can perform a restore operation on demand only.

Backup options

You can backup and restore the settings and service data of your BCM450.

During the backup procedure, you can exclude a number of optional services from the backup operation to ensure that service is not interrupted. The remainder of the services and settings are automatically included during a backup operation. The following table lists the components that you can choose to include or exclude from the backup operation.

Optional components

Component	Description
CallPilot Configuration	Includes Voice mail and Contact Center configuration information.
CallPilot Messages	Includes Voice mail and Contact Center configuration and Voice mail and Contact Center messages.
IP Music	Includes IP Music configuration.

Select the optional components that best fit your backup strategy. For example, if you do not want to backup personal voice mail messages, you can select the CallPilot Configuration component and clear the CallPilot Messages component, which saves all CallPilot information except for personal voice mail messages.

When you perform a restore operation, you can choose to restore any optional components included in the backup operation.

BCM450 backup file characteristics

When you perform a backup operation, the BCM450 creates a backup archive and stores it in a location that you specify. The archive file includes embedded archives, each of which represent a different part of the BCM450 system:

- archive.sig — ensures the integrity of all the data in the archive
- various archive files — contain the configuration settings and operating data

In addition to the configuration and application information, every backup operation includes the following files:

- Software Inventory — provides a snapshot of the software component release level
- Software History — provides a snapshot of the software history

These files document the system software level from which you took the backup. They are located in the archive softwarelevel.tar.gz.

Backup archives transferred to servers or to attached USB storage devices are named according to the system name of the BCM450, the date, and the time of the backup. Archives are prefixed with Bak_. For example, an archive created on July 8, 2005 at 1:52:55 pm is named Bak_acme-melbourne_20050708T135255.tar.

You can use only the most recent backup to the USB storage device for a restore operation. To access historical backup archives, attach the USB storage device to a personal computer and use the Restore from My Computer option.

Backup destinations

The following table lists the destinations to which you can back up data. Whichever destination you choose, the backup operation replaces the BCM copy of the archive, so that a copy of the most recent backup always remains on the BCM450. You can use this to restore your BCM450 without transferring a backup from an external device or server.

Backup destinations

Destination	Description
BCM	<p>For an immediate backup, saves backup archives to the hard drive of the BCM450.</p> <p>You cannot specify a path. Each backup overwrites any preexisting backup.</p>
My Computer	<p>For an immediate backup, saves backup archives to any accessible location on the client PC with the BCM450 Element Manager installed. You can specify a name for the backup, so that the system does not overwrite the preexisting backup.</p>
Network Folder	<p>Saves data to a shared network folder.</p> <p>The remote server must provide a Microsoft Windows-like shared file resource and a user account with rights to create and write files in the destination location. You cannot browse the network directories to select the destination folder, but you can specify a directory by identifying the path.</p>
FTP Server	<p>Saves backup archives to a File Transfer Protocol server.</p> <p>The system sends credentials and backup data without encryption. The remote server must provide an FTP server application and a user account with rights to allow the BCM450 to create and write files in the destination location.</p> <p>You cannot browse the FTP server to select the destination folder, but you can specify a directory by identifying the path.</p>
SFTP Server	<p>Saves backup archives to an SFTP server. This method encrypts the logon credentials and the data in transit.</p> <p>You must set up the remote SFTP server to allow the BCM450 to communicate with the SFTP server. When you set up an SFTP folder as a storage location on the network, you must use an SCP server. BCM450 supports OpenSSH 3.7.</p>
USB Storage Device	<p>Saves backup archives to a USB storage device.</p> <p>The system writes the files to the top directory level. You cannot specify a path to a different directory on the storage device. Format the USB storage device as FAT32.</p>

Attention: For backup files greater than 2.0G, you must choose My Computer or an SFTP server as the backup destination.

Before you back up BCM450 data, make sure that the BCM450 has appropriate access to the shared resource on which you will store the data. You must configure full access permissions on the shared resource.

Restore optional components

You can select the components which you want to restore.

You can restore a backup to a different system; for example, to quickly bring a second system into service in a new installation. In this case, not all of the configuration information in the Configuration backup is relevant to the second system. You can select whether to restore device-specific configuration information, such as network settings. You may wish to exclude certain components from restoration. For example, you can exclude the network settings from a restore operation to avoid giving two machines on your network the same identity.

When you restore from a backup archive, you can check the level of the software update of the archive file, and determine which updates you need to apply before you begin the restore operation. The `softwarelevel.tar.gz` file within the backup archive contains up to two text files: `installedsoftware.txt` and `history.log`. The `installedsoftware.txt` file is present at all times, while the `history.log` file is present only if software patches were applied to the BCM450 or if a software upgrade was performed. The `history.log` file contains the update history of the BCM450 at the time the backup archive was made. You can use this file to identify the software updates that you must apply to the target system before you perform the restore operation.

You should restore backup information only to another unit that has the same software release level. If the second unit has an older software release level, you can use the Reset button on the BCM450 front panel to reset the BCM450 unit to the factory default software level and default configuration settings. You can then apply software updates to bring the unit to the same software release level as that of the unit from which you took the backup.

The BCM450 verifies that the software release level of the unit to which you want to apply the backup is consistent with the software release level of the backup file. If the BCM450 detects a potential issue, the BCM Element Manager provides you with an error message.

Impact on system resources

A restore operation is a service-affecting operation. A number of services that run on the BCM450 system stop and then restart after the data restores. The BCM450 displays a reboot warning if any of the components selected for restoration require a system restart. The following table lists the effects of restoring optional components.

Effects of a restore operation on the system

Component	Effect
Core Telephony	Service interruption.
IP Telephony	Service interruption.
Keycodes	Reboots the device.
Data Services and Network interfaces	Network interruption.
Security	Service interruption. Replaces SSL certificate.
CallPilot Messages	Service interruption. Existing voice messages are lost.
CallPilot Configuration	Service interruption. Existing voice messages are lost.
Media Services Manager	Service interruption.
Core Telephony	Service interruption.

Restore operations and logs

All backup and restore operations are logged. To view this activity, retrieve the Operational Logs and examine the file called archiver.systemlog.

Log management

This section provides information about log management on the BCM450 system.

Log management navigation

- [Overview of BCM450 logs \(page 54\)](#)
- [Log types \(page 55\)](#)
- [Transferring and extracting logs \(page 57\)](#)
- [Log Browser \(page 58\)](#)

Overview of BCM450 logs

A log archive is a collection of individual log events generated by the BCM450. An administrator can use log archives to monitor and analyze system behavior, user sessions, and events. You manage logs by transferring selected BCM450 log archives from the BCM450 to a specified location, such as your personal computer. You can then view individual log events using the Element Manager Log Browser or your usual text editor.

Attention: Depending on the privileges assigned to you, you may or may not see all the log files or processes described in this chapter.

In addition to the log files generated by the BCM450 the Element Manager itself generates a log file. This log is found under the File selection of the Element Manager toolbar. This log contains diagnostic information. The BCM450 manages log archives and maintains generations of information depending upon size or other criteria. Generations of log files have a numbered extension such as 3.gz. A generation of the alarms.systemlog file is created each time the BCM450 is rebooted or when the log file reaches the 1 MB limit.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Log types

The BCM450 logs are grouped in three categories:

- Operational logs
- Diagnostic logs
- Sensitive logs

Each log category contains one or more log files. A log transfer groups all selected categories into a common archive. The embedded categories have easily identified names and are accessible to utilities such as WinZip (MS-Windows) and tar (UNIX).

When you transfer log archives, a set of additional log files is included in the log archive. These files are system information reports, which contain information about the system at the time of the log transfer.

Administrators have access to all log categories. Users who need only operational information have access to Operational and System Information logs.

Log type navigation

- [Operational logs \(page 55\)](#)
- [Diagnostic logs \(page 56\)](#)
- [Sensitive logs \(page 56\)](#)

Operational logs

Operational logs contain information about the BCM450 system and its use, such as alarm information, configuration changes, and security information. Administrators and authorized users can access Operational logs and view them using the Log Browser.

[Operational logs \(page 56\)](#) lists the log files that belong to the Operational logs category.

Operational logs

Log type	Log name	Description
Alarm log	alarms.systemlog	Records alarms that were written to the Element Manager alarm panel. Other possible alarms, if they cannot be viewed using the BCM450 Element Manager, are logged in the alarms diagnostic log.
Configuration change	configchange.systemlog	Records Element Manager configuration data changes by user and time
Security log	security.systemlog	Records users logging in and out as well as locked out users
	psmtest.systemlog	Records Ethernet interface activity and hard drive
	psmOMS.log	Records platform status, such as operational
Archive log	archiver.systemlog	Records backup, restore, and log management activity
Activity log	MonitGuard.systemlog	Records MonitGuard activity, an application that monitors main BCM services and applications.
	psmtest.systemlog	Records Ethernet interface activity and hard drive partitions.

Diagnostic logs

Diagnostic logs contain the log files generated by the BCM450 software components. These log files are required only if additional system information is requested by Nortel Technical Support to help diagnose a BCM450 issue. Only an administrator can access Diagnostic logs.

Sensitive logs

Sensitive logs may contain sensitive customer information, such as personal identification numbers or bank account and credit card numbers. Users may enter sensitive information using their telephone sets, for example when performing telephone banking.

Sensitive logs are grouped in a separate category to allow the administrator to decide whether to include this category of log files in a log file transfer, depending on the nature of the connection being used for the transfer. Administrators may choose to exclude Sensitive logs when the network or the destination is not sufficiently secure or when there are other privacy or security concerns.

The Sensitive Logs category includes only three log files for core telephony, LAN CTE, and Voice CTI.

Attention: The Sensitive Logs category can become very large due to the large core telephony log files.

Attention: Once logs are transferred to an external location, the administrator is responsible for securing the information and controlling access to it.

Additional system information

A set of System Information files is included with every log file transfer. These are reports rather than log files, and contain a snapshot of operating state of the BCM450 system at the time of the log file transfer. These reports are automatically collected and included with every log file transfer.

The files included in this category are .txt files. You can open these files with an application such as Word Pad or Microsoft Word, but you cannot open or view them using the Element Manager Log Browser. Nortel recommends Word Pad, since this application retains the column structure of the logs.

Transferring and extracting logs

Using the BCM450 Element Manager, you can transfer log files by using:

- an immediate log transfer
- a scheduled log transfer

You can create, modify, or delete a scheduled log transfer.

You can transfer log files to the following destinations:

- a USB storage device
- your personal computer
- a network folder
- an FTP server
- an SFTP server for secure file transfer

Log archives transferred to servers and the USB device are named with a Log_ prefix. The system name of the BCM450 and the date/time are appended to the prefix. An example filename is Log_acme_20050708T101604.tar.

When you transfer log files to the computer on which your Element Manager is installed, the default location for the Logs folder is \BCM450ElementManager\files\logs\. You may wish to create a folder within this folder for each BCM you are managing, so that log files from a particular BCM450 can always be transferred to the associated log file folder on your computer.

When you are transferring the log archive to your personal computer, you may also wish to save the log archive file using the system name and date as part of the file name. This will simplify the task of locating the tar file later. For example, you may wish to save the tar file as “Log_acme20050315.tar”.

You use the BCM450 Element Manager to transfer log files from the BCM450 to an external location. You must transfer the log files to an external device before you can view them. If you are using the BCM450 Element Manager Log Browser to view the logs, you will also have to extract the log files from the log archive that is transferred from the BCM450. The log archive contains a collection of log files.

When you transfer the log archives to another device, you can specify:

- the location to which you want to transfer log files, such as your personal computer or a network folder
- the category of logs you want to transfer, such as Sensitive Information logs
- a schedule for a log file transfer

You can also transfer log files using the BCM450 Web page if you cannot access the BCM450 Element Manager.

After you transfer the log archives, several options are available to you for extracting the log file information and for viewing the log files. If you are using the BCM450 Element Manager (recommended), the Log Browser prompts you to extract the actual log files from the .tar file. If you prefer, you can use the WinZip application to expand the .tar file into its included log files. As an alternative to using the Element Manager Log Browser, you can use an application such as WordPad to view the log files.

Using the BCM450 Element Manager Log Browser to view extracted log files gives you the ability to view information in a way that suits you; for example, you can filter and sort information according to priority, time, message, and so on.

Log Browser

The Log Browser is an application that you can use to search for and view information about log events from different types of data sources. You can determine what type of information you want to see and customize how you want to display the information.

Log Browser navigation

- [Log Browser overview \(page 59\)](#)
- [Retrieval Criteria area \(page 59\)](#)
- [Retrieval Results list \(page 61\)](#)
- [Log Details area \(page 62\)](#)

Log Browser overview

You can view the following log files using the Element Manager Log Browser:

- all log files of type .systemlog
- most log files of type .log
- log files of type .txt or other file extensions that cannot be viewed using the Log Browser

You can use an application such as WordPad or Microsoft Word to view log files that you cannot view using the Log Browser.

[Table 14 Log files and the Log Browser \(page 59\)](#) lists the log files that you can view using the Log Browser.

Table 14 Log files and the Log Browser

Log File	Can be viewed in the Log Browser?
Operational logs (.systemlog)	Yes
Diagnostic logs	Some can
System Information	No
Sensitive Information	No

The Log Browser contains the following areas:

- Retrieval Criteria area
- Retrieval Results list
- Log Details area

Retrieval Criteria area

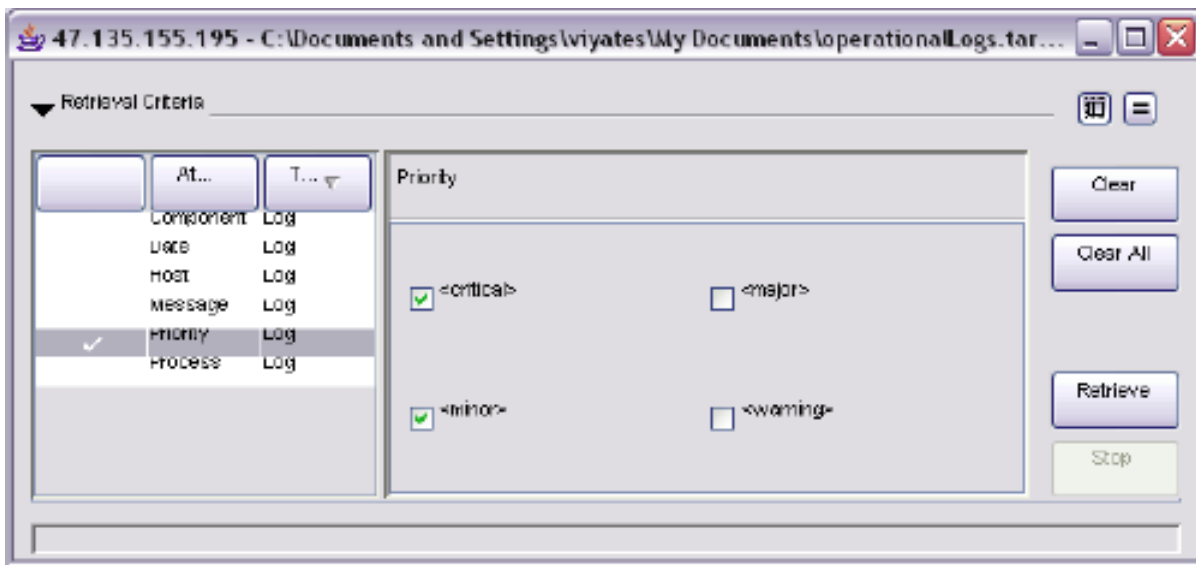
The Retrieval Criteria area at the top of the Log Browser window displays a list of network element and alarm attributes that you can use to define the criteria for browsing a selected log file.

You can display or close the Retrieval Criteria area by clicking on the arrow to the right of the Retrieval Criteria field.

Retrieval criteria area specific to the log file that you are viewing. For example, .log files with four columns have four possible retrieval criteria, while .systemlog files with six columns have six possible retrieval criteria. You can define the criteria for browsing log files by selecting or deselecting criteria.

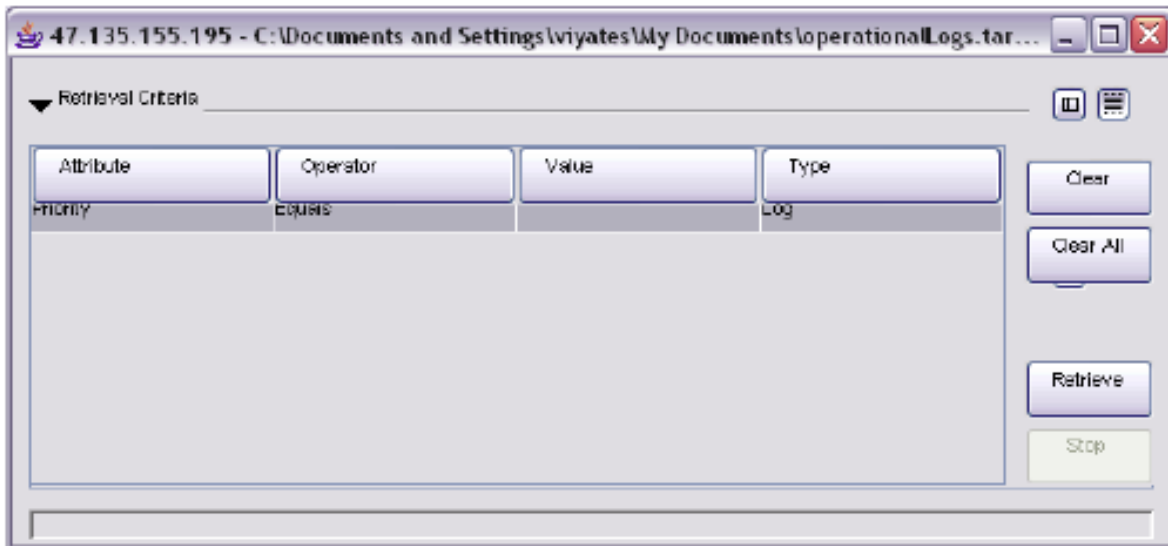
When you select an attribute from the Retrieval Criteria table, the Criteria Definition area to the right of the table displays the corresponding details for the attribute you selected. You can select or define the corresponding details.

Figure 2 Criteria Definition area



You can click the Pane View buttons at the top right corner of the Retrieval Criteria area to display a summary view of your selected criteria. This allows you to review selected criteria before you retrieve the logs.

Figure 3 View selected criteria



After you select an attribute, you can click the Clear button to remove it from the summary list, click the Clear All button to remove selected attributes, or click the Retrieve button to initiate a retrieval of log files according to the criteria you defined in the Retrieval Criteria area.

Retrieval Results list

The Retrieval Results area displays the list of log information that was retrieved according to the criteria you selected in the Retrieval Criteria area. The information is displayed in a table that you can sort by clicking column headings.

While the Log Browser is retrieving records, you can monitor the progress of the retrieval by following the progress counter. This counter also displays the elapsed time and the number of records found. You can stop the retrieval by clicking the Stop button.

The Log Browser displays all the records it has found, to a set maximum display limit. The maximum display limit is 3000 records. Most log files exceed this limit; when this happens, you cannot view the remaining records in the log file. If this is the case, try using filter criteria for a specific date or dates to reduce the number of results.

You can sort the contents of the table by clicking the headings in the table. You can view details about a log record by selecting a log record or multiple log records in the Retrieval Results area.

To filter information displayed in the Retrieval Results table, you can select or clear the check boxes in the Show area below the Retrieval Results table. You can filter the results by alarm severity: Debug, Info, Warn, or Error.

Log Details area

The Log Details area located below the Retrieval Results list displays the details for a selected log record or multiple log records.

Hardware inventory

This section provides information about hardware inventory on the BCM450 system.

The BCM450 Hardware Inventory panel provides information about the BCM450 physical system. There are three tabs on the main Hardware Inventory panel:

- **System**—Provides information about the key components of the BCM450.
- **Devices**—Provides information about any non-BCM450 components connected to the system.
- **Additional information**—Provides manufacturer details about the BCM450.

You can view information, and you can also add information about certain devices, such as an asset ID and location information, to facilitate tracking of the BCM450 hardware inventory in asset management systems.

You can view the information in the Hardware Inventory remotely, using Simple Network Management Protocol (SNMP) management systems and the Entity Management Information Base (MIB), RFC2737.

Software updates and software inventory

During the lifecycle of the BCM450, you can apply software updates to the BCM450 unit to introduce new functionality. Between software upgrades, you may find it necessary to apply software updates to resolve field issues. Both software upgrades and software updates are applied in the same manner. Using the BCM450, you can:

- obtain software updates from different storage locations, such as an FTP site or USB storage device
- view the software upgrade and update history of the BCM450
- apply and, in some cases, remove software updates
- view the software inventory of the BCM450
- apply software updates at a scheduled time

BCM450 software is organized into software components that you can individually update as required. The version of each software component is tracked so that you can determine the exact software release level of a BCM450 to the component level. You can view the complete inventory of

software installed on the BCM450. The Software Inventory table displays all the software components installed on the system, the functional group and the software version of each component.

BCM450 utilities

This section contains information about the utilities that are part of the Element Manager. These utilities provide information about the BCM450 system, so that you can monitor and analyze system status and performance. The BCM450 utilities are:

- Ping
- Trace Route
- Ethernet Activity
- Reset
- Diagnostic Settings
- IP Set Port Details

For information about the BCM Monitor utility, also available through Element Manager, see [BCM Monitor \(page 66\)](#).

Ping

Ping (Packet InterNet Groper) is a utility that you can use to verify that a route exists between the BCM450 and another device. Ping sends an ICMP (Internet Control Message Protocol) echo request message to a host. It expects an ICMP echo reply, which you can use to measure the round-trip time to the selected host. You can measure the percent packet loss for a route by sending repeated ICMP echo request messages.

Attention: Establishing a PPP link over a modem may take some time. If the Ping utility times out before the modem call can be established, click the Ping button again.

Trace Route

You can use Trace Route to measure round-trip times to all hops along a route. This helps you to identify bottlenecks in the network. Trace Route uses the IP time-to-live (TTL) parameter to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL value of 0 or 1. Instead, a router discards the packet and returns to the originating IP address an ICMP time exceeded message.

Trace Route sends an IP datagram with a TTL of 1 to the selected destination host. The first router to handle the datagram sends back a time exceeded message. This message identifies the first router on the route. Trace Route then transmits a datagram with a TTL of 2.

The second router on the route returns a time exceeded message until all hops are identified. The Trace Route IP datagram has a UDP Port number not likely to be in use at the destination (normally greater than 30 000). The destination returns a port unreachable ICMP packet. The destination host is identified.

Ethernet Activity

The Ethernet Activity panel is a utility that you can use to view ethernet activity in the BCM450 system.

Reset

You can use the Reset utility to:

- reboot the BCM450 system
- perform a warm reset of telephony services
- perform a cold reset of telephony services
- shut down the system

The following table lists the Reset functions.

Reset functions

Function	Description	Impact
Reboot BCM450 System	Restarts the operating system of the BCM450 system	Temporarily stops all services on the system. Restarts all services. This operation does not affect configuration parameters or programming.
Warm Reset Telephony Services	Restarts telephony services running on the BCM450 system	Restarts all telephony services, including LAN CTE, voice mail, and IP telephony. This operation does not affect configuration parameters or programming.

Reset functions

Function	Description	Impact
Cold Reset Telephony Services	Resets telephony programming of the BCM450 system to the factory defaults for that software level	<p>Affects all telephony services, including LAN CTE, voice mail, and IP telephony.</p> <p>Telephony services restart with all telephony programming at default values for the specified region, template, and start DN, for the current software release level.</p> <p>A cold reset erases voice message mailboxes and messages if the DN length is not set to system defaults.</p> <p>For information about setting the DN length, refer to the BCM450 Device Configuration Guide.</p>
System Shutdown	Shuts down the BCM450.	Stops all services in preparation for removing power from the system.

Diagnostic Settings

Diagnostic settings is a utility that allows you to determine the level of system reporting you require for released ISDN or VoIP calls. You can choose to have no text, a simple explanation, or a detailed explanation.

IP Set Port Details

The IP Set Port Details panel displays the settings for the physical ports that the IP sets connect to on the media bay modules.

The following table lists the fields on the IP Set Port Details panel.

Reset functions

Variable	Description
Port	The port number of the physical device.
DN	Each port supports one telephone, hence, one DN record.
Device type	The type of module.

Reset functions

Variable	Description
State	This field indicates whether a module line or DN is in use or even provisioned. States are: Idle Active Deprovisioned
Addon	
Addon	Indicates auxiliary items added to the telephony devices or trunks. This is a list number.
Type	This field indicates the type of add-on, such as a KIM module.
Version	This field indicates the version of firmware running on the add-on device.

BCM Monitor

BCM Monitor is a stand-alone diagnostic application that the system administrator uses to view real-time system and IP telephony information about BCM450 systems.

BCM Monitor is included with the installation of the Element Manager. You do not need to download the utility, unless you are an administrative user who requires access to only this management tool, and you do not have or require the Element Manager.

Using BCM Monitor, you can monitor the following:

- overall system status
- IP telephony functions of the BCM450 system, including IP device activity and VoIP session information
- utilization of resources
- operation of telephony applications (for example, Voice Mail and Contact Center)
- lines
- PRI, BRI, and IP trunks

The following operating systems support BCM Monitor:

- Microsoft Vista Business, Microsoft Vista Ultimate, and Microsoft Vista Enterprise. Both the 32-bit and 64-bit versions of Windows Vista are supported, except for limitations described in *System Overview* (NN40160-103).
- Windows 2000
- Windows XP
- Citrix

You use BCM Monitor from a remote PC that has IP connectivity to the monitored system. You can open multiple instances of BCM Monitor on a single PC to monitor several remote BCM450 systems at the same time.

When BCM Monitor connects to a BCM system that does not support a particular information element, this is indicated by “N/A” in the relevant BCM Monitor panes.

BCM Monitor does not require significant hard disk space or memory on the client PC.

System Administrators and support personnel can use BCM Monitor to obtain real-time troubleshooting data about the BCM system and to save data to generate system utilization and traffic reports.

BCM Monitor—BCM Info tab

The BCM Info tab displays static information about the BCM450 system, such as

- information about the main hardware components of the BCM450 system
- software installed on the system
- IP configuration data

You can use the information on this tab to verify the software release level of the BCM450, the published IP address and default gateway of the BCM450 main unit, the last time the BCM450 was rebooted, as well as IP address information about other Ethernet interfaces on the BCM450 main unit.

The installed devices on the BCM450 Info tab appear as follows:

- NIC: eth0 — indicates a LAN internal to the BCM450 system.
- NIC: eth1 — indicates a LAN accessible to the customer through ports 1, 2, and 3 on the front panel of the BCM450 main unit.
- NIC: eth2 — OAM LAN: a dedicated OAM port accessible as port 0, the leftmost Ethernet port on the front panel of the BCM450 main unit.

BCM Monitor—Media Card tab

The Media Card tab provides information about the telephony system of the BCM450. This tab provides the following information for a BCM450:

- the hardware of the BCM450 main unit on which the telephony software resides
- the telephony software component release level and market profile
- configuration information, such as media channels (64 kbits/s B channels), and the total number of logical DSP resource units
- the available tasks and tasks in service

The Media Card tab provides the following information for BCM systems:

- Media Card hardware, including type and revision, and voice bus channels
- Media Card firmware, including core load and market profile
- configuration information, such as DS30 configuration, dialup WAN, media channels (64 kbits/s B channels), signaling channels (D channels), processor expansion cards, and the total number of logical DSP resource units
- multiple DSPs and the tasks that are available and in-service for each

BCM Monitor—Voice Ports tab

The Voice Ports tab displays real-time information about configured voice ports. A configured voice port is a logical device used for voice mail, and Contact Center. Values associated with voice ports change with the usage of the switch, and are therefore well suited for dynamic logging to view trends relating to system activity.

You can use the Voice Ports tab to view the following information:

- information about voice ports used by the Voice CTI services, such as the resource limit and how many voice CTI ports are enabled and assigned
- how many Voice CTI ports are assigned to Contact Center and voice mail
- how many assigned ports are currently active, and the DN of the user assigned to the port
- voice port details, which show information about activity on each enabled voice port

BCM Monitor—IP Devices tab

The IP Devices tab displays information about call activity associated with IP sets, wireless sets, and IP trunks. IP sets include IP clients (for example, the i2050 softphone), i200x IP sets, and wireless sets.

The IP Devices tab shows how many sets in each category are enabled, connected, and active. The tab displays the DN, IP address, and type of set for each active call.

BCM Monitor—RTP Sessions tab

The RTP Sessions tab displays information about Real Time Protocol (RTP) over UDP sessions, which involve either the BCM450 system or an IP set controlled by the BCM450 system.

You can use the information in this tab to monitor the direct path between two IP sets.

The tab displays information about

- local IP endpoints (two sets both connected to the BCM450)
 - combinations of IP to IP, TDM to IP, and TDM to TDM
 - an estimate of network traffic generated by RTP sessions between TDM devices or local IP devices
- local to remote IP endpoints
 - combinations of IP to IP, TDM to IP
 - an estimate of network traffic generated by RTP sessions
- remote IP endpoints (IP to IP)
 - an estimate of network traffic generated by RTP sessions between remote IP endpoints
- the number of allocated media gateways that are providing a connection between a TDM device and an IP endpoint

The RTP Sessions tab also displays detailed information about active RTP sessions. The RTP Session Details area displays the following line for each active session:

```
IP Endpoint A}{IP Trunk X}<stream info>{IP Trunk Y}{IP  
Endpoint B} Codec FPP Details
```

The IP Endpoint tokens contain information about each IP endpoint (type, DN, IP address, RTP port number). The IP Trunk tokens contain information about the IP Trunk used by each endpoint (if no trunk is used, the token is omitted). The Stream Info token shows which RTP streams are enabled between the two endpoints. The Codec token describes the codec type used for the RTP session. The FPP shows the negotiated value of frames per packet. The Details token shows additional information about the RTP session.

BCM Monitor can display real-time RTP session statistics for sessions that involve at least one media gateway. These statistics include information about duration of the session, the number of bytes and packets sent or received per second and per session. You can use these statistics for troubleshooting packet loss or routing problems.

BCM Monitor—UIP tab

The UIP tab displays information about Universal ISDN Protocol (UIP) activity associated with IP trunks (MCDN messages), BRI loops, and PRI loops on the BCM450.

You can monitor UIP modules by:

- enabling or disabling monitoring of MCDN over IP messages for calls made over IP trunks
- selecting and configuring a bus used by expansion modules
- selecting the type of ISDN module connected to the expansion unit
- enabling or disabling monitoring of loops on BRI modules connected to the expansion unit

UIP message details

The Universal ISDN Protocol Messages section displays a folder for each UIP module that you enable for monitoring. Each folder displays up to 20 most recent UIP messages. You can expand UIP messages that contain at least one information element. An information element can contain data, which you can expand as well.

Each UIP message line contains the following information:

- the direction in relation to the BCM450 (> for incoming or < for outgoing)
- the message type (CC for Call Control, MTC for Maintenance)
- the direction in relation to the call reference origin (> Cref Origin for incoming or < CRef Origin for outgoing)
- the message name (or a hexadecimal value if the name is unknown)
- additional data extracted from information elements

BCM Monitor—Line Monitor tab

The Line Monitor tab shows the status of lines on the BCM450 system. You can view the number of active lines, and view all lines on the BCM450 system, including inactive lines.

For all lines displayed in the line monitor area, you can view the following information:

- direction — “Outgoing” indicates that the call originated from the BCM450; “Incoming” indicates that the call originated from outside and is directed at the BCM450
- start time — displays the time and date on which the call started
- user — displays the DN and name of the BCM450 user
- state — displays “Idle” if there is no active call on the line; displays “Dialing” if the BCM450 user is in the process of dialing digits to place a call; displays “Alerting” if a call has been received on the line and a BCM450 user’s phone is ringing; displays “Connected” if the line has a connected call; displays “Held” if the line has a call on hold.
- duration — displays the duration of the call
- number and name — displays the line number and line name

In the line monitor area, colors are used to indicate the state of each line:

- gray represents lines that are idle
- blue represents lines that are active
- red represents lines that are alerting
- dark red represents lines that are on hold

BCM Monitor—Usage Indicators tab

The Usage Indicators tab displays real-time information about the BCM450 system.

The tab displays the following information:

- BCM450 system data, including CPU and memory use
- resources used on the Media Card, including signaling channels, media channels, voice bus channels, and DSP resources
- active telephony devices, such as IP trunks, IP sets, voice ports, and media gateways

The information is displayed as an absolute figure and as a percentage of the resource used. You can capture a static snapshot of this information or log it dynamically.

Usage values

The Usage Indicators tab can show high CPU usage occurring on the BCM450. When you create backup archives or log archives, a high level of CPU usage can occur. This level of CPU usage is normal during backup and log management operations.

Usage values are accompanied by a colored bar. The following table describes the usage value indicators and recommended actions.

Table 15 Usage value indicators

Indicator color	Indicator meaning	Recommended action
Green	Usage values are normal.	None.
Yellow	Potential resource problem.	Further investigation is recommended if an indicator remains yellow for an extended period.
Red	Critical resource problem.	Further investigation is recommended if an indicator remains red for more than a few seconds.

Statistical values

BCM Monitor stores the minimum and maximum values for many of the statistics that appear on BCM Monitor tabs. A statistic must be a numeric value and must change over time; that is, the value cannot be a static value. Examples of statistics that have minimum and maximum values are CPU usage, Active Lines, and Enabled i20XX sets. Examples of statistics that do not have minimum and maximum values are Dial-up WAN (which is not a numeric value) and Serial Number (which is static).

The values that BCM Monitor displays are the minimum and maximum values for the current BCM Monitor session. The minimum and maximum values are reset when you exit the BCM Monitor.

The three values remain on the Status bar until you select another value. These values also continue to change as the value for the selected statistic changes. Use this if you want to monitor a single statistic on one panel while you are viewing the information on another panel.

When BCM Monitor stores the minimum and maximum value, it also stores the date and time when the minimum or maximum occur.

You can do the following with statistical values:

- view minimum and maximum values
- view the date and time of minimum and maximum values
- reset minimum and maximum values

System-wide security policies configuration

Configure system-wide security policies to install web server certificates and to download the SSK key-pair.

System-wide security policies configuration navigation

- [BCM450 system entry policy definition \(page 73\)](#)
- [BCM450 local authentication policy definition \(page 74\)](#)
- [BCM450 authentication service policy definition \(page 77\)](#)
- [BCM450 SSL and SSH policy usage \(page 81\)](#)

BCM450 system entry policy definition

Use the Entry Policy tab to perform the following procedure:

Configuring system access control policy

Configure system access control policies to allow the administrator to set system access rules.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Entry Policy .
2	To prevent the warning message from opening after log on, select the Disable post-login check box. OR To allow the warning message to appear, leave the Disable post-login check box cleared.
3	Enter a new warning in the Post-login message box or leave the default warning.
4	Select the Disable Telset login check box to prevent users from administrating the system through any Telset interface.

- 5 In the **Challenge Key** field, enter a new Challenge key or use the default Nortel Challenge key provided.
If you enter a new Challenge key, keep a record of it.
- 6 Select the **Show/Hide** check box to display asterisks rather than the characters in the Challenge key.

--End--

BCM450 local authentication policy definition

Define authentication policies to control password length and complexity, to configure the number of times a user can attempt to log in, and how often users must renew their passwords.

This section contains information on the following topics:

- [Configuring credential complexity \(page 74\)](#)
- [Configuring lockout on failed login policy \(page 75\)](#)
- [Configuring the idle session timeout \(page 75\)](#)
- [Configuring password expiry policy \(page 76\)](#)
- [Configuring password history policy \(page 76\)](#)

Configuring credential complexity

Configure credential complexity to allow the administrator to define the rules for password length and password complexity.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Local Authentication Policy .
2	In the Credential Complexity section, in the Credential Type column, select the credential type.
3	In the Minimum User ID Length column, enter the required number of characters or digits for a user ID.
4	Under the Minimum Password Length column, enter the required number of characters or digits for the user password.

- 5 Under the **Password Complexity Level** column, enter a number from 1 to 5 that represents the password complexity level requirement (or enter 0 for no complexity check).

For an alphanumeric password, the level is from 0 to 4. For a numeric password, the level is from 0 to 5.

--End--

Configuring lockout on failed login policy

Configuring Lockout on Failed Login allows the administrator to set lockout rules. Administrators can unlock accounts that have been locked out

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Local Authentication Policy .
2	In the Lockout on Failed Login section, select the Enable lockout check box to enable lockout capabilities.
3	In the Lockout counter field, enter a number that represents the number of times a user can try to log on with an incorrect password.
4	In the Lockout duration field, enter the number of minutes the user becomes locked out after the Lockout counter threshold is reached.
5	In the Lockout counter reset field, enter the number of minutes to wait to reset the Lockout counter.

--End--

Configuring the idle session timeout

You can use the idle session timeout feature to automatically log out users who have been inactive for a specified period of time. Follow this procedure to specify the period of time before inactive sessions are timed out.

Procedure steps

Step	Action
1	Select Configuration > Administrator Access > Security Policies > Session Management Policy .
2	In the Session timeout box, enter the number of minutes to wait after a period of inactivity before the session times out.

--End--

Configuring password expiry policy

Use this procedure to create a password expiry policy.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Local Authentication Policy .
2	Select the Enable check box to enable the password expiry policy.
3	In the Days before password expire field, enter the number of days that you can use a password before it expires.
4	In the Warning days before password expire field, enter the number of days prior to password expiry that the user receives a notification.

--End--

Configuring password history policy

You can use the password history feature to prevent users from re-using the same password. Administrators can configure the number of previous passwords to store and check.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Local Authentication Policy .
2	In the Password history section, select the Enable Password History check box.

- 3 In the **Password history length** field, enter the number of previous passwords to store and check for an account.

--End--

BCM450 authentication service policy definition

Use the following procedures to define BCM450 authentication service policies

BCM450 authentication service policy definition procedures navigation

- [Configuring the authentication method \(page 77\)](#)
- [Configuring the authentication server \(page 78\)](#)

Configuring the authentication method

By default, users are authenticated on the local Nortel Business Communications Manager 450 1.0 system. In a network with multiple Nortel Business Communications Manager 450 1.0 systems, you can choose to authenticate users on a centralized server using Remote Authentication Dial-In User Service (RADIUS).

The BCM RADIUS client complies with the RADIUS protocol described in RFC 2865, and supports the following authentication and authorization functions:

- ACCESS-REQUEST messages
- ACCESS-ACCEPT messages

RADIUS does not support other functions, such as challenge key and accounting messages.

If you use RADIUS to authenticate and authorize users, and the RADIUS servers are not in-service or are out-of-contact, the BCM reverts to using local authentication.

When you select RADIUS as the authentication method, user IDs and passwords are authenticated on the RADIUS server for the following tasks:

- administration of the BCM using Element Manager
- access to the BCM website
- access to the BCM Monitor
- dial-in access to the BCM using modem or ISDN
- Contact Centre administration
- BCM Amp configuration
- CTE DA ProAE

- Telset administration
- IP set registration
- voice mail and web-based administration
- Call Detail Recording functionality

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Authentication Service Policy .
2	On the Account Management menu, select Local Authentication or RADIUS .
--End--	

Configuring the authentication server

To authenticate users on a centralized RADIUS server, you must configure the server using Element Manager.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > Authentication Service Policy .
2	To select a server as the primary authentication server, click in each column of the table and enter the following attributes:

Column	Value
Server name	Name of the server to use for authentication
Server IP address	IP address of the server to use for authentication
Server Port	Port number of the server to use for authentication
Enabled	Select to enable the use of RADIUS server authentication
In Contact	Read-only. Indicates whether the BCM450 is in contact with the RADIUS server.
Details for RADIUS server	
Server Message Timeout	Length of time to wait for the server to respond to a request for authentication before timing out

Column	Value
Server Retries	Number of times to retry connecting with the primary server before using an alternate means of authenticating the user
Server Shared Secret	Key required for the BCM450 to communicate with the authentication server

- 3 Repeat [step 2](#) to configure the secondary server.

--End--

Vendor specific attributes

The BCM requires Vendor Specific Attributes (VSAs) to be present in RADIUS client requests. The BCM Webpage provides a RADIUS dictionary that defines the Nortel-specific attributes. The attributes in the dictionary are defined for a Funk RADIUS server; however, the RADIUS client in BCM complies with RFC 2865 and can be used on other RADIUS servers.

Procedure steps

Step	Action
1	Configure the ACCESS-REQUEST message. In an ACCESS-REQUEST message, the BCM will look for the attributes listed in the table below.

Attribute Name	Description
NAS Identifier	The hostname of the BCM (string)
IP	The IP address of the BCM
Calling Station ID	The IP address/DN of the client attempting the request

- 2 Configure the ACCESS-ACCEPT message. In an ACCESS-ACCEPT message, the BCM will look for the attributes listed in the table below.

Attribute Name	Value	Description
RADIUS attribute type	26	Vendor specific attribute
Vendor type	562	Northern Telecom (Nortel)

Attribute Name	Value	Description
Vendor attribute type	166	BCM privilege level of the user being authenticated. Enter this level as a hex integer.
Privilege level	0-36 (see Table in step 3)	Privilege level of user, entered in big endian (network byte order).

- 3** Configure the privilege levels. BCM requires the RADIUS server to provide one or more privilege levels when the user authentication is accepted. The table below lists the privilege levels. These must be provided as a 32-bit integer in big endian format (network byte order).

Privilege Name	Value	Description
VoiceMailAdmin	0	Voice Mail Administrator
Contact Center	1	MMCC - Administrator
SBAInstaller	2	Set Based Administrator Level 4
SBASystemCoord	3	Set Based Administrator Level 3
SBASystemCoordBasic	4	Set Based Administrator Level 2
SBABasic	5	Set Based Administrator Level 1
Security	6	Security Administrator
CTEApp	7	LAN CTE DA Pro AE User
SBA - IP Set Registration	8	IP set registration privilege - from IP telephone sets
Application - BCMMonitor	9	BCM Monitor user
CDRApp	10	CDR Application Privilege
Modem Login	11	Dial-in PPP user
GuestLogin	12	Access to BCM Web pages - user level
AdminDownload	13	Administrative application download
ExclusiveAccess	14	Access to the BCM when exclusive access flag enabled.
Admin	16	Access to the BCM configuration.
DataAdmin	17	Access to the data portion of CIM/ XML interface.

Privilege Name	Value	Description
RemoteAccess	18	Access to remote access fields of BCM configuration.
Guest	19	Access to all of the BCM configuration for read-only access.
VoiceAdmin	20	The ability to administer the telephony portion of the BCM configuration.
BackupOperator	21	The ability to backup a BCM.
RemoteMonitoring	22	The ability to remotely connect to and manage the BCM configuration (ie. SNMP configuration).
SoftwareUpgrade	23	The ability to upgrade the BCM
AlarmViewer	24	The ability to view the alarm screen.
Operational Logs	26	The ability to download operational logs.
Diagnostic Logs	27	Full access to download any logs.
ISDN - Dial-in	30	The ability to use ISDN for dial-in.
WAN - Dial-in	32	The ability to use WAN for dial-in PPP access.
System - Serial Port	36	The ability to configure the BCM through the serial port.

--End--

BCM450 SSL and SSH policy usage

Use SSL and SSH policies to upload custom security certificates and to ensure secure connections for backup and restore operations and software updates.

BCM450 SSL and SSH policy usage procedures navigation

- [Uploading a Web Server Certificate \(page 82\)](#)
- [Transferring an SSH Key-Pair \(page 82\)](#)

Uploading a Web Server Certificate

You can upload a private security certificate to replace the generic web certificate provided with Nortel Business Communications Manager 450 1.0. With a custom site-specific certificate, you can have site validation that eliminates security warnings.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > SSL and SSH Policy .
2	In the SSL section, click Install Web Server Certificate .
3	On the Transfer Certificate browse pane, locate and select the security certificate file.
4	Click Transfer Certificate .
5	On the Transfer Private Key browse pane, locate and select the private key file.
6	Click Transfer Private Key .
7	On the Install Web Server certificate window, click OK to install the certificate.

--End--

Transferring an SSH Key-Pair

Transfer an SSH Key-Pair to allow the administrator to download a public security certificate or an SSH key-pair. Install the new certificate on each SFTP server the BCM450 communicates with to ensure a secure connection for operations, such as backup and restore, and software updates.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Security Policies > SSL and SSH Policy .
2	In the SSH section, click Generate New SSH Key-pair . The new key is placed on the computer running BCM450.
3	Click Save .
4	For the SSH Key-pair, click Transfer Public Key .
5	In the Save dialog box, locate and select the public key file.

6 Click **Save** to transfer the files.

--End--

Accounts, groups, and privileges configuration

This chapter provides procedures to establish accounts and access privileges for users of the Nortel Business Communications Manager 450 1.0 system

Navigation

- [BCM450 user account management \(page 85\)](#)
- [BCM450 feature additions for dial-up users \(page 88\)](#)
- [BCM450 user password management \(page 90\)](#)
- [BCM450 user group management \(page 91\)](#)
- [BCM450 account enabling and disabling \(page 94\)](#)

BCM450 user account management

Use the following procedures to create, modify, delete, and configure user accounts.

BCM450 user account management procedures navigation

- [Adding a new user account \(page 85\)](#)
- [Modifying a user account \(page 86\)](#)
- [Adding Telset access for a user \(page 87\)](#)
- [Deleting a user account \(page 87\)](#)

Adding a new user account

Administrators can create user accounts when the BCM is configured to authenticate users locally. The BCM450 supports up to 1999 user accounts.

After you create a new user account, you can assign groups to that account. Groups are sets of privileges based on user tasks or roles. For information about creating groups and assigning groups to accounts, see [BCM450 user group management procedures navigation \(page 91\)](#) and [Adding a user account to a group \(page 93\)](#).

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account tab.
2	Click Add .
3	In the Add Account dialog box, enter a description of the account in the Description field.
4	Enter the user identifier in the User ID field.
5	In the User password field, enter the user password.
6	In the Confirm password dialog box, enter the user password again.
7	Enter the Telset user ID.
8	In the Telset password field, enter the Telset password for the user.
9	In the Confirm password dialog box, enter the user password again.
10	If the user connects through a modem, enter the number the system dials to contact the client modem in the Modem Callback Number field and a passcode in the Modem Callback Passcode field (include the correct routing codes).
11	If the user connects through ISDN, enter the number the system dials to contact the client in the ISDN Callback Number field and a passcode in the ISDN Callback Passcode field.
12	Select the Change Password on Login check box to force a password change when the user logs on to Element Manager.
13	Select the Change Password on Login Telset check box to force a password change when the user logs on to Telset.
14	Click OK to save the user account.
15	After the account is created, the user can change their own password through the Current Account pane.

--End--

Modifying a user account

As an administrator, you can modify user accounts.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account tab.

- 2 Select an existing user in the **Accounts** table and click **Modify**.
- 3 In the **Modify Account** dialog box, make the changes you require.
- 4 Click **OK** to save the user account.

--End--

Adding Telset access for a user

As an administrator, you can provide an existing user with access to the system through a set-based connection.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account tab.
2	Select an existing user on the Accounts table and click Modify .
3	In the Telset User ID field, enter the user identifier.
4	In the Telset Password field, enter the user Telset password.
5	Reenter the Telset password in the Confirm Password dialog box.
6	Click OK .

--End--

Deleting a user account

As an administrator, you can delete user accounts.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account tab.
2	Select a user on the Accounts table.
3	Click Delete .
4	In the Confirmation box, click Yes to remove the user account from the system.

--End--

BCM450 feature additions for dial-up users

Use the following procedures to add features for dial-up users.

BCM450 feature additions for dial-up users procedures navigation

- [Adding callback for a dial-up user \(page 88\)](#)
- [Adding NAT rules for a dial-up user \(page 88\)](#)

Adding callback for a dial-up user

As an administrator, you can provide callback access to a user who accesses the system through a dial-up connection.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account > Remote Access tab.
2	Select an existing user on the Accounts table.
3	Click the Modify button in the Accounts section.
4	If the user connects through a modem, enter the number the system dials to contact the client modem in the Modem Callback Number field and enter a passcode in the Modem Callback Passcode field (include the correct routing codes).
5	If the user is connecting through ISDN, enter the number the system dials to contact the client in the ISDN Callback Number field and enter a passcode in the ISDN Callback Passcode field.
6	Click OK .
--End--	

Adding NAT rules for a dial-up user

As an administrator, you can add Network Address Translation (NAT) rules for a user who accesses the system through a dial-up connection. When you add a NAT rule, your network can use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. This translation provides security for your LAN by hiding the IP addresses of devices on your network from external computers. This procedure allows you to configure NAT on dial-up interfaces.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Account .
2	Select an existing user on the Accounts table.
3	Click the Remote Access tab.
4	Click Modify in the NAT Rules section.
5	In the Rule 1: Dial-in Side field, enter the IP address to be translated from. You cannot use a multicast address when you create NAT rules.
6	In the LAN Side field to the right, enter the IP address on the local LAN to be translated to. You cannot use a multicast address when you create NAT rules.
7	Repeat step 5 and step 6 to create additional rules.
8	Click OK .

--End--

BCM450 user password management

Use these procedures to manage user passwords.

BCM450 user password management procedures

- [Changing a user password \(page 90\)](#)
- [Changing the current user password \(page 91\)](#)

Changing a user password

As an administrator, you can change a user's forgotten password, or reset the user password for each user to enforce regular password-change policy. You can also force a password change when the user logs in.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Accounts tab.
2	Select the user record from the table and click Modify .
3	In the Modify Account window, delete the asterisks in the Password or Telset password field.
4	Enter a new password and click OK .

- 5 Reenter the password in the **Confirm Password** dialog box.
- 6 Provide the user with this password and request that they change it as soon as possible through the **Current User** pane or click on **Change Password on Login** to make a password change mandatory.

--End--

Changing the current user password

As a user or an administrator, you must change your password periodically.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > Current Account pane.
2	Select the password field that needs to change.
3	Enter a new password that conforms with the system password policies, defined by the administrator during system setup. A Password Confirmation dialog box appears.
4	In the Password Confirmation dialog box, enter the new password again.
5	Click OK . The password takes effect the next time you log on.

--End--

BCM450 user group management

Use the following procedures to manage and create user groups.

BCM450 user group management procedures navigation

- [Creating a group \(page 92\)](#)
- [Deleting a group \(page 92\)](#)
- [Modifying group privileges \(page 92\)](#)
- [Adding a user account to a group \(page 93\)](#)
- [Deleting a user account from a group \(page 93\)](#)

Creating a group

As an administrator, you can create new groups to satisfy organizational requirements.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Groups tab.
2	Click Add .
3	In the Add Group dialog box, enter a name for the new group.
4	Click OK .
5	Select the new group from the Groups list.
6	In the Group Privileges section, click Add .
7	In the Add Privilege to Group dialog box, select one or more group privileges to assign to the group and click OK .

--End--

Deleting a group

As an administrator, you can delete groups as organizational requirements change.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Groups tab.
2	Select a group and click Delete .
3	Click Yes on the Confirmation box to remove the groups from the list.

--End--

Modifying group privileges

You can only modify user-created groups; you cannot modify default group privileges.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Groups tab.
2	Select a group.
3	Click the General tab.
4	Click the Group Privileges tab.
5	Select one or more group privileges
6	Click Delete to remove the privileges from the existing group. OR Click Add to add the privileges to the existing group.
7	In the Confirmation dialog box, click Yes .

--End--

Adding a user account to a group

As an administrator, you can add user accounts to one or more groups to satisfy access requirements.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Groups tab.
2	Select a group and click the Members tab.
3	Click Add .
4	In the Add Account to Group dialog box, select one or more groups.
5	Click OK .

--End--

Deleting a user account from a group

As an administrator, you can remove user accounts from a group to limit user access.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Groups tab.
2	Select a group and click the Members tab.
3	Select one or more groups in Accounts in Group in the Members table.
4	Click Delete .
5	In the Confirmation box, Click OK to remove the groups from the list.

--End--

BCM450 account enabling and disabling

This section contains information on enabling and disabling user accounts.

BCM450 account enabling and disabling procedures navigation

- [Deleting a user account from a group \(page 93\)](#)
- [BCM450 account enabling and disabling procedures navigation \(page 94\)](#)
- [Enabling and disabling an account \(page 95\)](#)

Reenabling a locked-out user

As the administrator you can re-enable a locked-out user when the user has exceeded the login retry threshold.

The system shows an enabled check box under the **Locked Out** column on the **Users** table.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Accounts tab.
2	Select the user record with the Locked Out status check box selected.
3	Clear the Locked Out check box.

--End--

Enabling and disabling an account

As the administrator, you can enable or disable accounts on an immediate or timed basis.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , choose Configuration > Administrator Access > Accounts and Privileges > View by Accounts tab.
2	Select the user you want to disable or enable in the Accounts table.
3	Under the Disabled column, either select (disable) or clear (enable) the check box for the user. The change applies the next time the user logs on.

--End--

Data backup and restore

This chapter provides instructions for backup and restore operations for Nortel Business Communications Manager 450 1.0.

Navigation

- [On-demand backups \(page 97\)](#)
- [Scheduled backups \(page 102\)](#)
- [Data restoration \(page 111\)](#)

On-demand backups

This section contains information on how to perform on-demand backups to the BCM450.

On-demand backup procedures navigation

- [Performing an immediate backup to your BCM450 \(page 97\)](#)
- [Performing an immediate backup to your personal computer \(page 98\)](#)
- [Performing an immediate backup to a network folder \(page 99\)](#)
- [Performing an immediate backup to a USB storage device \(page 100\)](#)
- [Performing an immediate backup to an FTP server \(page 100\)](#)
- [Performing an immediate backup to an SFTP server \(page 101\)](#)

Performing an immediate backup to your BCM450

You can perform immediate backups to BCM450.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup . The Backup pane opens and displays the Immediate Backup tab.
3	In the Backup To field, select BCM .

- 4 Click **Backup**.
- 5 The **Backup** window appears.
- 6 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 7 Click **OK**.
- 8 A warning window opens. Read the warning carefully, then click **Yes** to proceed.
- 9 A progress window appears. When the backup completes, the **Backup Complete** message appears.
- 10 Click **OK**.

--End--

Performing an immediate backup to your personal computer

You can perform immediate backups to your personal computer.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup .
3	The Backup pane appears and displays the Immediate Backup tab.
4	In the Backup To field, select My Computer .
5	Click Backup .
6	The Backup window appears.
7	In the Optional Components table, select or clear the check box for each component to include or exclude these components from the backup operation.
8	Click the OK button.
9	A warning message appears. Read the warning then, click Yes to proceed.
10	A progress window appears. When the backup preparation is complete, the Save window appears.
11	Specify the directory and enter a file name in the File Name field.
12	Enter a file name with a .tar extension (e.g. backup2.tar) so that you can examine the file with a utility such as WinZip. If you do not select the folder backup, the new backup file is stored in the root of this folder.

- 13 Click **Save**.
When the backup is complete the **Backup Complete** message appears.
- 14 Click **OK**.

--End--

Performing an immediate backup to a network folder

You can perform immediate backups to network folder.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup .
3	The Backup pane appears and displays the Immediate Backup tab.
4	In the Backup To field, select Network Folder .
5	Configure the Network Folder attributes.
6	Click the Backup button.
7	The Backup window appears.
8	In the Optional Components table, select or clear the check box for each component to include or exclude these components from the backup operation.
9	Click OK .
10	A warning window opens. Read the warning carefully, then click Yes to proceed.
11	A progress window appears. When the backup preparation is complete, the Backup Complete message displays.
12	Click OK .

--End--

Performing an immediate backup to a USB storage device

You can perform immediate backups to a USB storage device.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup .
3	The Backup pane appears and displays the Immediate Backup tab.
4	In the Backup To field, select USB Storage Device .
5	Click Backup .
6	The Backup window appears.
7	In the Optional Components table, select or clear the check box for each component to include or exclude these components from the backup operation.
8	Click the OK button.
9	A warning message appears. Read the warning then, click Yes to proceed.
10	A progress window appears. When the backup preparation is complete, the Backup Complete message appears.
11	Click OK .
--End--	

Performing an immediate backup to an FTP server

You can perform immediate backups to an FTP server.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup .
3	The Backup pane appears and displays the Immediate Backup tab.
4	In the Backup To field, select FTP Server .
5	Configure the FTP Server attributes.
6	Click Backup . The Backup window appears.

- 7 In the **Optional Components** table, select or clear the check box for each component to include or exclude these components from the backup operation.
- 8 Click **OK**.
- 9 A warning window opens. Read the warning carefully, then click **Yes** to proceed.
- 10 A progress window appears. When the backup is complete, the **Backup Complete** message displays.
- 11 Click **OK**.

--End--

Performing an immediate backup to an SFTP server

You can perform immediate backups to an SFTP server.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Under the Task Navigation Panel , click on the Administration tab. |
| 2 | Open the Backup and Restore folder, and then click Backup . |
| 3 | The Backup pane opens and displays the Immediate Backup tab. |
| 4 | In the Backup To field, select SFTP Server . |
| 5 | Configure the SFTP Server attributes. |
| 6 | Click Backup . The Backup window appears. |
| 7 | In the Optional Components table, select or clear the check box for each component to include or exclude these components from the backup operation. |
| 8 | Click OK . |
| 9 | A warning window opens. Read the warning carefully, then click Yes to proceed. |
| 10 | A progress window appears. When the backup preparation is complete, the Backup Complete message displays. |
| 11 | Click OK . |

--End--

Scheduled backups

You can create scheduled backups in order to perform backups at a date and time that you choose. For example, you can choose a date and time during which your business is closed. This will avoid disrupting the normal work-day routine and may allow your backup file to transfer more quickly.

Scheduled backup procedures navigation

- [Accessing the schedule of regular backups \(page 102\)](#)
- [Modifying scheduled backups \(page 102\)](#)
- [Deleting scheduled backups \(page 103\)](#)
- [Creating a scheduled backup to BCM \(page 104\)](#)
- [Creating a scheduled backup to a network folder \(page 105\)](#)
- [Creating a scheduled backup to a USB storage device \(page 107\)](#)
- [Creating a scheduled backup to an FTP server \(page 108\)](#)
- [Creating a scheduled backup to SFTP server \(page 109\)](#)

Accessing the schedule of regular backups

You can view existing scheduled backups.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder
3	Click Backup .
4	The Backup pane appears and displays the Immediate Backup tab.
5	Click the Scheduled Backups tab.
6	The Scheduled Backups pane appears. Existing scheduled backups appear in the Scheduled Backups table.
--End--	

Modifying scheduled backups

You can modify the following existing scheduled backup components:

- the memo for the scheduled backup
- optional components to include in the backup
- schedule details for the backup

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Backup .
4	The Backup panel opens and displays the Immediate Backup tab.
5	Click the Scheduled Backups tab.
6	The Scheduled Backups panel opens.
7	Select a scheduled backup in the Scheduled Backups table.
8	Click Modify.
9	The Modify Scheduled Backup window appears.
10	Modify the attributes of the scheduled backup as required.
11	Click OK .
12	The modified backup appears in the Scheduled Backups table.

--End--

Deleting scheduled backups

You can delete existing scheduled backups.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Backup .
4	The Backup pane appears and displays the Immediate Backup tab.
5	Click the Scheduled Backups tab.
6	The Scheduled Backups pane appears.
7	Select a scheduled backup in the Scheduled Backups table.

- 8 Click **Delete**.
A confirmation window appears.
- 9 Click **Yes**.
The scheduled backup is removed from the **Scheduled Backups** table.

--End--

Creating a scheduled backup to BCM

You can create scheduled backups to BCM.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Under the Task Navigation Panel , click on the Administration tab. |
| 2 | Open the Backup and Restore folder, and then click Backup .
The Backup pane appears and displays the Immediate Backup tab. |
| 3 | Click the Scheduled Backups tab. |
| 4 | The Scheduled Backups pane appears. |
| 5 | Click Add . |
| 6 | The Add Scheduled Backup window appears. |
| 7 | In the Backup To field, select BCM . |
| 8 | Click OK . |
| 9 | The Add Scheduled Backup window opens. Read the warning carefully before proceeding. |
| 10 | In the Optional Components table, select or clear the check box to include or exclude these components from the backup operation. |
| 11 | Click OK . |
| 12 | Configure the schedule attributes. |
| 13 | Click OK .
The scheduled backup is displayed in the Scheduled Backups table. |

--End--

Variable definitions

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often you want the scheduled backup to occur. Options include: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays selections for the month and day of the month. If you select Weekly, days of week are display. Select the check box for Daily to select the day.
Month	Select the month in which you want the scheduled backup to occur. Displays only when you select Once as the Recurrence.
Day of Month	Select the day of the month that you want the scheduled backup to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time that you want the scheduled backup to occur.

Creating a scheduled backup to a network folder

You can create scheduled backups to a network folder.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Backup . The Backup pane appears and displays the Immediate Backup tab.
4	Click the Scheduled Backups tab. The Scheduled Backups pane appears.
5	Click the Add button. The Add Scheduled Backup window appears.
6	In the Backup To field, select Network folder.
7	Configure the Network folder attributes.

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and resource name. For example, \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password of the user.
Directory	Enter the path to the subdirectory (optional).

8 Click **OK**.

The **Add Scheduled Backup** window appears.

9 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.

10 Configure the schedule attributes.

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often you want the scheduled backup to occur. Options are: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays for the month and day of the month. If you select Weekly, the days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month that you want the scheduled backup to occur. Displays only when you select Once as the Recurrence.
Day of Month	Select the day of the month that you want the scheduled backup is to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time that you want the scheduled backup is to occur.
Recurrence	Select how often you want the scheduled backup to occur. Options are: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, the days of the week are displayed. Select the check box for Daily to select the day.

- 11 Click **OK**.

The scheduled backup is displayed in the Scheduled Backups table.

--End--

Creating a scheduled backup to a USB storage device

You can create scheduled backups to a USB storage device.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Backup . The Backup pane appears and displays the Immediate Backup tab.
4	Click the Scheduled Backups tab. The Scheduled Backups pane appears.
5	Click Add . The Add Scheduled Backup window appears.
6	In the Backup To field, select USB Storage Device .
7	Click OK . The Add Scheduled Backup window opens.
8	In the Optional Components table, select or clear the check box to include or exclude these components from the backup operation.
9	Configure the schedule attributes.

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often you want the scheduled backup to occur. Options are: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, the days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month that you want the scheduled backup to occur. Displays only when you select Once as the Recurrence.

Attribute	Action
Day of Month	Select the day of the month that you want the scheduled backup is to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time that you want the scheduled backup to occur.

10 Click **OK**.

The scheduled backup is displayed in the **Scheduled Backups** table.

--End--

Creating a scheduled backup to an FTP server

You can create scheduled backups to an FTP server.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder, and then click Backup .
3	The Backup panel opens and displays the Immediate Backup tab.
4	Click the Scheduled Backups tab.
5	The Scheduled Backups panel opens.
6	Click the Add button.
7	The Add Scheduled Backup window opens.
8	In the Backup To field, select FTP Server .
9	Configure the FTP Server attributes.

Attribute	Action
FTP Server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the user name on the FTP server.
Directory	Enter the path to the subdirectory (optional).

10 Click **OK**.

- 11 The **Add Scheduled Backup** window appears.
- 12 In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 13 Configure the schedule attributes.

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often you want the scheduled backup to occur. Options are: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays selections for the month and day of the month. If you select Weekly, the days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month that you want the scheduled backup to occur. Displays only when you select Once as the Recurrence.
Day of Month	Select the day of the month that you want the scheduled backup to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time that you the scheduled backup is to occur.

- 14 Click **OK**.
The scheduled backup is displayed in the **Scheduled Backups** table.

--End--

Creating a scheduled backup to SFTP server

You can scheduled backups to SFTP server.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Under the Task Navigation Panel , click on the Administration tab. |
| 2 | Open the Backup and Restore folder. |
| 3 | Click Backup . |
| 4 | The Backup pane appears and displays the Immediate Backup tab. |
| 5 | Click the Scheduled Backups tab. |

- 6** The Scheduled Backups pane opens.
- 7** Click **Add**.
- 8** The **Add Scheduled Backup** window opens.
- 9** In the **Backup To** field, select SFTP Server.
- 10** Configure the FTP Server attributes.

Attribute	Action
SFTP Server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Password	Enter the password associated with the user name.
Directory	Enter the path to the subdirectory (optional).

- 11** Click **OK**.
- 12** The **Add Scheduled Backup** window opens.
- 13** In the **Optional Components** table, select or clear the check box to include or exclude these components from the backup operation.
- 14** Configure the schedule attributes.

Attribute	Action
Memo	Enter a note for the scheduled backup, as applicable.
Recurrence	Select how often you want the scheduled backup to occur. Options are: Once, Daily, Weekly, and Monthly. Depending on the option you choose, the window displays selections for the month and day of the month. If you select Weekly, days of the week are displayed. Select the check box for Daily to select the day.
Month	Select the month that you want the scheduled backup to occur. Displays only when you select Once as the Recurrence.
Day of Month	Select the day of the month that you want the scheduled backup to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time that you want the scheduled backup to occur.

- 15 Click **OK**.

The scheduled backup is displayed in the **Scheduled Backups** table.

--End--

Data restoration

You can restore BCM450 configuration and application data using the Element Manager.

Data restoration procedures navigation

- [Restoring a backup from BCM \(page 111\)](#)
- [Restoring a backup from a PC \(page 112\)](#)
- [Restoring a backup from a network folder \(page 113\)](#)
- [Restoring a backup from USB storage \(page 114\)](#)
- [Restoring a backup from an FTP server \(page 115\)](#)
- [Restoring a backup from an SFTP server \(page 116\)](#)
- [Restoring the factory default configuration \(page 117\)](#)

Restoring a backup from BCM

You can restore backups from the BCM.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Restore .
4	The Restore pane appears. The Restore From field has BCM as the default value.
5	Click Restore .
6	The Select Components to Restore window appears.
7	Select the optional components that you want to include from the backup file.
8	Click OK .
	A warning window opens and displays information about components that will be affected by the restore operation.

- 9 Click **Yes** to proceed.
A progress window opens. When the operation completes, the **Restore Complete** window appears.
- 10 Click **OK**.

--End--

Restoring a backup from a PC

You can restore a backup from a PC.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Under the Task Navigation Panel , click on the Administration tab. |
| 2 | Open the Backup and Restore folder, and then click Restore .
The Restore pane appears. |
| 3 | In the Restore From field, select My Computer . Click Restore .
The Open window appears. |
| 4 | Select the backup file to restore. |



CAUTION

Risk of service loss

When you proceed to the next step, the selected file overwrites the backup file stored on the Nortel Business Communications Manager 450 1.0. Ensure that you select the correct backup file before you proceed.

- 5 Click **Open**.
The **Select Components to Restore** window appears.
A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the BCM450.
- 6 Select the optional components that you want to include from the backup file.
- 7 Click **OK**.
A warning window opens and displays information about components that will be affected by the restore operation.


- 8 Click **Yes** to proceed
A progress window appears. When the operation completes, the **Restore Complete** window appears.
- 9 Click **OK**.

--End--

Restoring a backup from a network folder

You can restore a backup from a network folder.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Restore . The Restore pane appears.
4	In the Restore From field, select Network Folder.
5	Configure the Restore from Network Folder attributes. A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the Nortel Business Communications Manager 450 1.0.
<div><div>CAUTION Risk of service loss When you proceed to the next step, the selected file overwrites the backup file that is stored on the Nortel Business Communications Manager 450 1.0. Ensure that you select the correct backup file before you proceed.</div></div>	
6	Click Open . The Select Components to Restore window appears.
7	Select the optional components that you want to include from the backup file.
8	Click OK . A warning window opens and displays information about components that will be affected by the restore operation.

- 9 Click **Yes** to proceed.
A progress window appears. When the operation completes, the **Restore Complete** window appears.
- 10 Click **OK**.

--End--

Variable definitions

Attribute	Action
Network Folder	Enter the hostname or IP address of the network folder and resource name. For example, \\<server>\<resource>.
User Name	Enter the user name associated with the network folder.
Password	Enter the password of the user.
Directory	Enter the path to the subdirectory, as applicable (optional).
File	Enter the name of the backup file.

Restoring a backup from USB storage

You can restore a backup from a USB storage device.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Under the Task Navigation Panel , click on the Administration tab. |
| 2 | Open the Backup and Restore folder.
Click Restore .
The Restore pane appears. |
| 3 | In the Restore From field, select USB Storage Device . |
| 4 | Select the backup file to restore. |

- 5 A window opens and displays information about the backup file, including a warning that the selected backup file will replace the backup file currently stored on the Nortel Business Communications Manager 450 1.0.

**CAUTION****Risk of service loss**

When you proceed to the next step, the selected file overwrites the backup file that is stored on the Nortel Business Communications Manager 450 1.0. Ensure that you select the correct backup file before you proceed.

- 6 Click **Open**.
- 7 The **Select Components to Restore** window appears.
- 8 Select the optional components that you want to include from the backup file.
- 9 Click **OK**.
- 10 A warning window opens and displays information about components that will be affected by the restore operation.
- 11 Click **Yes** to proceed.
A progress window opens. When the operation completes, the **Restore Complete** window opens.
- 12 Click **OK**.

--End--

Restoring a backup from an FTP server

You can restore a backup from an FTP server.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Restore . The Restore pane appears.
4	In the Restore From field, select FTP Server .
5	Configure the Restore from FTP Server attributes.

Attribute	Action
FTP server	Enter the hostname or IP address of the FTP server.
User Name	Enter the user name associated with the FTP server.
Password	Enter the password associated with the user name.
Directory	Enter the path to the subdirectory, as applicable (optional).
File	Enter the name of the backup file.

**CAUTION****Risk of service loss**

When you proceed to the next step, the selected file will overwrite the backup file that is stored on the Nortel Business Communications Manager 450 1.0. Ensure that the correct backup file is selected before proceeding.

- 6 Click **Open**.
- 7 The **Select Components to Restore** window appears.
- 8 Select the optional components that you want to include in the backup file.
- 9 Click **OK**.
A warning window opens and displays information about components that will be affected by the restore operation.
- 10 Click **Yes** to proceed.
A progress window opens. When the operation completes, the Restore Complete window opens.
- 11 Click **OK**.

--End--

Restoring a backup from an SFTP server

You can restore a backup from an SFTP server.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.

- 3 Click **Restore**.
- 4 The **Restore** pane appears.
- 5 In the **Restore From** field, select **SFTP Server**.
- 6 Configure the Restore from SFTP Server attributes.

Attribute	Action
SFTP server	Enter the hostname or IP address of the SFTP server.
User Name	Enter the user name associated with the SFTP server.
Password	Enter the password associated with the user name.
Directory	Enter the path to the subdirectory, as applicable (optional).
File	Enter the name of the backup file.

**CAUTION****Risk of service loss**

When you proceed to the next step, the selected file overwrites the backup file that is stored on the Nortel Business Communications Manager 450 1.0. Ensure that you select the correct backup file before you proceed.

- 7 Click **Open**.
The **Select Components to Restore** window appears.
- 8 Select the optional components that you want to include in the backup file.
- 9 Click **OK**.
A warning window opens and displays information about components that will be affected by the restore operation.
- 10 Click **Yes** to proceed.
A progress window opens. When the operation completes, the **Restore Complete** window appears.
- 11 Click **OK**.

--End--

Restoring the factory default configuration

You can restore the factory default configuration.

Procedure steps

Step	Action
1	Under the Task Navigation Panel , click on the Administration tab.
2	Open the Backup and Restore folder.
3	Click Restore . The Restore pane appears.
4	In the Restore From field, select Factory Default .
5	Click the Restore button. The Select Components to Restore pane appears.
6	Select the optional components that you want to include from the backup archive.
7	Click OK . A warning window opens and displays information about components that will be affected by the restore operation.
8	Click Yes to proceed. A progress window opens. When the operation completes, the Restore Complete window opens.
9	Click OK .

--End--

BCM450 log management system

This section describes how to view and manage logs generated by the BCM450 system.

BCM450 log management system navigation

- [Performing immediate log transfers \(page 119\)](#)
- [Configuring scheduled log transfers \(page 124\)](#)
- [Transferring log files using the BCM450 Web Page \(page 128\)](#)
- [Using the Log Browser \(page 130\)](#)
- [Viewing log files using other applications \(page 133\)](#)

Performing immediate log transfers

This section contains information on the following topics:

- [Performing an immediate log transfer to a USB storage device \(page 119\)](#)
- [Performing an immediate log transfer to a personal computer \(page 120\)](#)
- [Performing an immediate log transfer to a network folder \(page 121\)](#)
- [Performing an immediate log transfer to an FTP server \(page 122\)](#)
- [Performing an immediate log transfer to an SFTP server \(page 123\)](#)

Performing an immediate log transfer to a USB storage device

Use the following procedure to transfer a log to a USB storage device.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the Logs folder, and then click the Log Management task. The Log Management panel opens.
3	Click the Immediate Log Transfer tab.
4	In the Transfer To selection field, select USB Storage Device .
5	Click the Transfer button. A window opens.
6	Select the log file categories that you want to include in the log file transfer. All the log files associated with the selected categories will be transferred.
7	Click the OK button. A transfer window opens and displays applicable warnings.
8	Click the Yes button to initiate the transfer. The Progress Update window opens. When the log files are transferred, the Transfer Complete window opens.
9	Click the OK button. The log archive is saved in the location you specified.

--End--

Performing an immediate log transfer to a personal computer

Use the following procedure to transfer a log to your personal computer.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the Logs folder, and then click the Log Management task. The Log Management panel opens.
3	Click the Immediate Log Transfer tab.

- 4 In the **Transfer To** selection field, select **My Computer**.
- 5 Click the Transfer button.
A window opens.
- 6 Select the log file categories that you want to include in the log file. Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 7 Click the **Yes** button to initiate the transfer.
When the log archive is ready to be saved, the The Save window opens.
- 8 Select the directory in which you want to save the log file transfer.
- 9 In the **File Name** field, enter the name of the log file followed by a .tar extension. For example, log1.tar.

Attention: If you do not specify a .tar extension, the transfer proceeds and the file will be written to the specified location. The file, however, will be of an unknown type and your utilities may not operate with it. Rename the file with the extension .tar by right-clicking on the file and renaming it.

- 10 Click the **Save** button.
The Progress Update window displays while the files are being saved. When the files are saved, the Transfer Complete window opens.
- 11 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

--End--

Performing an immediate log transfer to a network folder

Use the following procedure to transfer a log to a network folder.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the Logs folder, and then click the Log Management task. The Log Management panel opens.
3	Click the Immediate Log Transfer tab.

- 4 In the **Transfer To** selection field, select **Network Folder**.
- 5 Configure the **Transfer to Network Folder** attributes.
- 6 Click the **Transfer** button.
The Transfer window opens.
- 7 Select the log file categories that you want to include in the log file transfer.
- 8 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 9 Click the **Yes** button to initiate the transfer.
The Progress Update window opens. When the log files are transferred, the Transfer Complete window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

--End--

Variable definitions

Column	Value
Network Folder	Hostname or IP address of the network folder and the resource name. For example, enter \\<server>\<resource>
User Name	User name associated with the network folder
Password	Password associated with the network folder
Directory	Path to the subdirectory, if applicable (optional)

Performing an immediate log transfer to an FTP server

Use the following procedure to transfer a log to an FTP server.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Click the Administration tab. |
| 2 | Open the Logs folder, and then click the Log Management task.
The Log Management panel opens. |

- 3 Click the **Immediate Log Transfer** tab.
- 4 In the **Transfer To** selection field, select **FTP Server**.
- 5 Configure the **Transfer to FTP Server** attributes.
- 6 Click the **Transfer** button.
The Transfer window opens.
- 7 Select the log file categories that you want to include in the log file transfer.
- 8 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 9 Click the **Yes** button to initiate the transfer.
The Progress Update window opens. When the log files are transferred, the Transfer Complete window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

--End--

Variable definitions

Column	Value
FTP Server	Hostname or IP address of the FTP server
User Name	User name associated with the FTP server
Password	Password associated with the FTP server
Directory	Path to the subdirectory, if applicable (optional)

Performing an immediate log transfer to an SFTP server

Use the following procedure to transfer a log to an SFTP server.

Attention: When you create a log archive, a high level of CPU usage may occur. This level of CPU is normal during a log management operation.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Click the Administration tab. |
| 2 | Open the Logs folder, and then click the Log Management task.
The Log Management panel opens. |
| 3 | Click the Immediate Log Transfer tab. |

- 4 In the **Transfer To** selection field, select **SFTP Server**.
- 5 Configure the **Transfer to SFTP Server** attributes.
- 6 Click the **Transfer** button.
The Transfer window opens.
- 7 Select the log file categories that you want to include in the log file transfer.
- 8 Click the **OK** button.
A confirmation window opens, and displays applicable warnings.
- 9 Click the **Yes** button to initiate the transfer.
The Progress Update window opens. When the log files are transferred, the Transfer Complete window opens.
- 10 Click the **OK** button.
The log file is saved as a .tar file in the location you specified.

--End--

Variable definitions

Column	Value
SFTP Server	Hostname or IP address of the SFTP server. For SFTP storage locations, you must use an SCP server. BCM450 supports Open SSH 3.7.
User Name	User name associated with the SFTP server
Password	Password associated with the SFTP server.
Directory	Path to the subdirectory, if applicable (optional)

Configuring scheduled log transfers

You can schedule a log transfer for a future date for a single transfer, or for recurring future transfers. You can create multiple schedule entries. For example, you can transfer Operational logs and System Information logs on a daily basis and transfer Diagnostic and Sensitive Information logs on a weekly basis.

This section contains information on the following topics:

- [Creating a scheduled log transfer \(page 124\)](#)
- [Modifying a scheduled log transfer \(page 126\)](#)
- [Deleting a scheduled log transfer \(page 127\)](#)

Creating a scheduled log transfer

Use the following procedure to schedule a log transfer.

Procedure steps

Step	Action
1	Click the Administration tab, and then open the Logs folder.
2	Click the Log Management task. The Log Management panel opens.
3	Click the Scheduled Log Transfer tab.
4	T he Scheduled Log Transfer panel opens.
5	Click the Add button. The Add Scheduled Transfer window opens.
6	In the Transfer To selection field, select the location to which you want to transfer the log files: <ul style="list-style-type: none"> • Network Folder • USB Storage Device • FTP Server • SFTP Server
7	Configure the Transfer To attributes.
8	Click the OK button. The Add Scheduled Transfer window opens.
9	In the Memo field, enter a description of the log transfer.
10	Select the log file categories that you want to include in the log file transfer.
11	Configure the schedule attributes.
12	Click the OK button. The scheduled log transfer is displayed in the Scheduled Log Transfer table.
	Note: If you select Network Folder, FTP Server, or SFTP Server as the Transfer To option, a Verify Connection Parameter dialog box displays. You can use this dialog box to test the connection to the destination, or continue without testing.

--End--

Variable definitions

Column	Value
Network Folder	Hostname or IP address of the FTP server
User Name	User name associated with the FTP server
Password	Password associated with the FTP server
Directory	Path to the subdirectory, if applicable (optional)

Variable definitions

Column	Value
Memo	Enter a note for the scheduled log transfer, as applicable.
Recurrence	Select how often the scheduled transfer is to occur. Options are: Once, Daily, Weekly, Monthly. Depending on the option you choose, the window displays selections for the month and day of month. If you select Weekly, days of the week check boxes appear so that you can select the days on which the transfer will occur.
Month	Select the month in which the scheduled transfer is to occur. Displays only when you select Once as the Recurrence.
Day of Month	Select the day of the month on which the scheduled transfer is to occur. Displays only when you select Once or Monthly as the Recurrence.
Time	Select the time at which the scheduled transfer is to occur. Click the field to display a Time box, where you can specify the hour, minute, second, and whether the time occurs in morning or afternoon. Close the box when you have finished specify the time.

Modifying a scheduled log transfer

Use the following procedure to modify a scheduled log transfer.

Procedure steps

Step	Action
1	Click the Administration tab, and then open the Logs folder.
2	Click the Log Management task. The Log Management panel opens.

- 3 Click the **Scheduled Log Transfer** tab.
- 4 In the **Scheduled Log Transfer** table, select a scheduled log file transfer.
- 5 Click the **Modify** button.
The Modify Scheduled Transfer window opens.
- 6 In the **Transfer To** field, modify the destination as appropriate.
- 7 In the **Memo** field, modify the memo for the scheduled log transfer as appropriate.
- 8 In the **Optional Components** area, modify the log file categories you want to include or exclude from the transfer, as appropriate.
- 9 Click the **OK** button.
The modified scheduled log transfer is displayed in the Scheduled Log Transfer table.

--End--

Deleting a scheduled log transfer

Use the following procedure to delete a log transfer that you have scheduled.

Procedure steps

Step	Action
1	Click the Administration tab, and then open the Logs folder.
2	Click the Log Management task. The Log Management panel opens.
3	Click the Scheduled Log Transfer tab.
4	In the Scheduled Log Transfer table, select a schedule.
5	Click the Delete button. A confirmation window opens.
6	Click the Yes button. The scheduled log transfer is deleted from the Scheduled Log Transfer table.

--End--

Transferring log files using the BCM450 Web Page

If you do not have access to Element Manager, you can transfer log files using the Web Page. When you use the BCM450 Web Page to transfer log files, you cannot choose the log file categories to transfer; all the log files in all the categories will be transferred.

This section contains information on the following topics:

- [Using the BCM450 Web Page to transfer logs to your personal computer \(page 128\)](#)
- [Using the BCM450 Web Page to transfer logs to other destinations \(page 129\)](#)

Using the BCM450 Web Page to transfer logs to your personal computer

Use the following procedure to transfer logs from the BCM450 Web Page to your personal computer.

Procedure steps

Step	Action
1	In your web browser, type the IP address of the BCM450 and click the Go button. The login screen opens.
2	Log in to the BCM450 using the same username and password that you use to log into the Element Manager. The BCM450 Web page opens.
3	Click the Administrators Applications link.
4	Click the BCM Logs link. The Retrieve Log Files panel appears.
5	Click one of the three options for file transfer: <ul style="list-style-type: none">• Transfer to My Computer• Store on USB Memory• Send to
6	If you select the Send to radio button, select a destination from the drop-down list, otherwise, go to the next step.
7	Click the Submit button at the bottom of the screen. A Working dialog box displays. When log retrieval is complete, the dialog box displays "Success."
8	Click the Click Here to Transfer Logs link. The File Download screen opens.

- 9 Click the **Save** button.
- 10 The **Save As** screen opens.
- 11 Specify the location where you want to save the log file transfer, and enter a name for the file in the **File Name** field.
- 12 Click the **Save** button.
The file is saved.

--End--

Using the BCM450 Web Page to transfer logs to other destinations

Use the following procedure to transfer logs from the BCM450 Web Page to any of the following destinations:

- a Windows shared folder
- an FTP server
- an SFTP server.

Procedure steps

Step	Action
1	In your web browser, type the IP address of the BCM450 and click the Go button. The login screen opens.
2	Log in to the BCM450 using the same user name and password that you use to log into Element Manager. The BCM450Web page opens.
3	Click the Administrators Applications link.
4	Click the BCM Logs link.
5	In the Retrieve Log Files area, select a destination for the retrieved logs: <ul style="list-style-type: none">• Transfer to my computer• Store on USB memory• Send to:
6	If you selected a Send To option, configure the destination attributes for the option you chose. The options are FTP, SFTP, or Windows Shared Folder.
7	Click the Submit button. A Working screen opens. When the log retrieval is complete, the screen displays "Done."

- 8 Click the **Click Here to Download Logs** link.
The File Download screen opens.
- 9 Click the **Save** button to save the backup.tar file.
The Save As screen opens.
- 10 Specify the location where you want to save the zipped file, and enter a name for the file in the **File Name** field. The file must have a .tar extension. For example, log2.tar.
- 11 Click the **Save** button.
The file is saved.

--End--

Variable definitions

Column	Value
Remote Resource	Enter the FTP or SFTP address or the network pathway, as appropriate. For SFTP storage locations, you must use an SCP server. BCM450 supports OpenSSH 3.7.
Directory	Enter the path of the directory to which you want to transfer the log files.
User ID	Enter the user ID associated with the remote resource.
Password	Enter the password associated with the remote resource. This option does not apply when the destination is an SFTP server.

Using the Log Browser

Once you have transferred log files using the Element Manager or the BCM450 Web page, you can extract the log files using the Element Manager Log Browser. You must extract the log files from the log archive before you can view them using the Element Manager Log Browser.

Prerequisites

Before you extract log files, create a folder in your directory for each archive and then follow the procedure [Extracting the log file \(page 131\)](#) to extract the archive into the appropriate folder.

Extracting the log file

Use the following steps to extract the log files from the log archive.

Procedure steps

Step	Action
1	Left-click a network element. The network element may be connected or disconnected.
2	Select File, View Network Element Logs . The View Log File window opens.
3	Select the directory or location that contains the transferred BCM450 log file tar archive.
4	Select Network Element log archives (*.tar) in the File of Type field.
5	Select the archive file, and then click the Open button. A confirmation dialog box opens.
6	Click the Yes button to extract the contents of the zipped file. A message dialog box opens and displays a success or error message for each extracted file.
7	Click the OK button to acknowledge an individual message, or click OK to All to acknowledge all messages once the extraction is complete. Alternatively, you can wait until the extraction is complete, and then close the window. Once the files are extracted, the View Log File window opens.
8	Select a log file folder, for example operationalLogs.tar. Select .systemlog from the Files of type field to show only log files that the Log Browser can display.
9	Click the Open button. The log file folder opens and the log files that it contains are displayed.
10	Select a .systemlog file or a .log file, and click the Open button. The Log Browser opens and displays retrieval results for the selected log file.
--End--	

Specifying retrieval criteria

Use the following steps to reset the status LED.

Procedure steps

Step	Action
1	In the Log Browser, ensure that the Retrieval Area is open by clicking on the arrow next to the Retrieval Criteria field.
2	In the Retrieval Criteria table, select an attribute.
3	The Criteria Definition area displays the corresponding details for the selected attribute.
4	Specify details for the selected attribute, as appropriate.
5	Click the Retrieve button. While the Log Browser is retrieving records, a progress counter displays the elapsed time and the number of records found. The results of the retrieval are displayed in the Retrieval Results list area.

--End--

Filtering retrieval results

The Log Browser displays all the records it has found, to a maximum display limit of 3000 records. Most log files exceed this limit; when this happens, you cannot view the remaining records in the log file. If this is the case, use filter criteria for a specific date or dates, or filter according to alarm severity, to reduce the number of results.

Procedure steps

Step	Action
1	In the Retrieval Results table, select or clear the checkboxes in the Show area.
2	To sort the contents of the Retrieval Results table, click on the table headings.

--End--

Viewing details for a single log record

Use the following steps to view details for a single log record.

Procedure steps

Step	Action
1	In the Retrieval Results list table, select a log record. Log details for the selected log record are displayed in the Log Details area.
--End--	

Viewing details for multiple log records

Use the following steps to view details for multiple log records.

Procedure steps

Step	Action
1	In the Retrieval Results list table, hold down the Shift key and select log records to select multiple contiguous log records. Log details for the selected log records are displayed in the Log Details area, separated by dashed lines.
2	In the Retrieval Results list table, hold down the Control key and select log records to select multiple non-contiguous log records. Log details for the selected log records are displayed in the Log Details area, separated by dashed lines.
3	To toggle between viewing log details for single and multiple log records separated by a dashed line, click the View Control buttons to the right of the Log Details area.
--End--	

Viewing log files using other applications

Using the Element Manager Log Browser to view log files enables you to control how you view log events by means of retrieval criteria and sorting tools. You can also view log files using other applications if the Element Manager is not available.:

- use WordPad to view .systemlog and .log files (tab delimited)
- open the files using Microsoft Word
- open the files using Microsoft Excel

BCM450 hardware inventory

This section describes how to use the hardware inventory to display and update information about BCM450 hardware.

BCM450 hardware inventory navigation

- [Viewing and updating information about the BCM450 system \(page 135\)](#)
- [Viewing information about devices \(page 142\)](#)
- [Viewing additional information \(page 143\)](#)

Viewing and updating information about the BCM450 system

This section contains information on the following topics:

- [Viewing and updating information about the main unit \(page 135\)](#)
- [Viewing expansion daughter card information \(page 136\)](#)
- [Viewing and updating information about media bay modules \(page 137\)](#)
- [Viewing information about hard disk drives \(page 138\)](#)
- [Viewing and updating system expansion information \(page 139\)](#)
- [Viewing and updating information about digital mobility controllers \(page 140\)](#)

Viewing and updating information about the main unit

Use the following procedure to view and update information about the main unit.

Procedure steps

Step	Action
1	In the BCM Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens and displays the BCM System tab.
3	View the information displayed in the BCM450 main unit area.

- 4 If you want to add or update the asset ID for the BCM450 main unit, enter an asset ID in the **Customer asset ID** field.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
System*	An arbitrary string that uniquely identifies the Physical Element and serves as the Element's key	Nortel BCM450 Communications Server	Read
Type*	The type of the physical entity	Chassis	Read
System name*	A user-friendly name for the object	System name of the BCM450	Read
System ID	A unique string that identifies this element	System ID which is Mac #1	Read
Model*	A textual description of the object	example 'BCM450 Telephony Only'	Read
Serial number	The serial number to the BCM450 unit	Nortel System Serial Number	Read
Customer asset ID*	Customer-defined tracking number	Initially zero	Write

Attention: Fields marked with an asterisk (*) can also be remotely queried by SNMP using the Entity MIB.

Viewing expansion daughter card information

Use the following procedure to view information about the expansion daughter card. The Expansion Daughter Cards area on the BCM System tab provides information about the daughter cards connected to the BCM main unit.

Procedure steps

Step	Action
1	In the BCM Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens, and displays the BCM System tab.

3 View the information displayed in the **Expansion Daughter Cards** area.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Location	The location of the expansion daughter card.	Alphanumeric	Read
Resource	The name or type of the expansion daughter card.	Alphanumeric	Read
FRU PEC Code	The PEC code of the field-replaceable unit.	Numeric	Read
FRU CPC Code	The CPC code of the field-replaceable unit.	Numeric	Read
Serial Number	The manufacturer's serial number of the field-replaceable unit.	Numeric	Read
Firmware Version	The firmware version of the unit.	Numeric	Read
Hardware Version	The hardware version of the unit	Numeric	Read
FRU	Indicates if the unit is considered field replaceable by the manufacturer.	True (if checked)	Read

Viewing and updating information about media bay modules

Use the following procedure to view information about the media bay modules. The Media Bay Modules area on the BCM System tab provides information about the MBMs connected to the BCM main unit.

Procedure steps

Step	Action
1	In the BCM Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens, and displays the BCM System tab.
3	View the information displayed in the Media Bay Modules area.
4	To update information about the media bay modules, enter an ID in the Asset ID field, and enter any other information in the Details field.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Instance	Specifies the location of the MBM.	Alphanumeric	Read
Resource	The name or type of the MBM.	Alphanumeric	Read
Asset ID*	Customer defined tracking number	Initially zero	Write
Details	Enter optional details about the MBM.	Numeric	Write
FRU	Indicates if the unit is considered field replaceable by the manufacturer.	True (if checked)	Read

Viewing information about hard disk drives

Use the following procedure to view information about the hard disk drives.

Procedure steps

Step	Action
1	In the BCM Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens, and displays the BCM System tab.
3	View the information displayed in the Hard Disk Drives area.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Instance	Identifies the location of the hard drive.	Numeric	Read
Resource	The type of hard disk installed.	Alphanumeric	Read
Order PEC Code	The PEC code of the hard drive.	Alphanumeric	Read
Serial Number	The serial number of the hard drive.	Alphanumeric	Read
Firmware version	The firmware version of the hard drive.	Alphanumeric	Read
FRU	Indicates if the unit is considered field replaceable by the manufacturer.	True (if checked)	Read

Viewing and updating system expansion information

Use the following procedure to view system expansion information. The BCM System Expansion area in the BCM System tab provides information about the expansion chassis.

Procedure steps

Step	Action
1	In the BCM Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory .

- The **Hardware Inventory** panel opens, and displays the **BCM System** tab.
- 3 View the information displayed in the **BCM System Expansion** area.
 - 4 To update information about the expansion chassis, click the **Present** checkbox to indicate that an expansion chassis is installed.
 - 5 To add a customer-defined asset number, enter an ID in the **Asset ID** field.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Resource	The name of the expansion chassis.	Alphanumeric	Read
Asset ID*	Customer defined tracking number	Initially zero	Write
Present	Indicates if an expansion unit to main unit is present	Yes (if checked)	Read
Field Replaceable	Indicates if the unit is considered field replaceable by the manufacturer.	True (if checked)	Read

Viewing and updating information about digital mobility controllers

Use the following procedure to view and update information about the digital mobility controllers.

Procedure steps

- | Step | Action |
|------|---|
| 1 | In the BCM Element Manager, connect to a BCM450 device. |
| 2 | Select Administration, General, Hardware Inventory .
The Hardware Inventory panel opens, and displays the BCM System tab. |
| 3 | View the information displayed in the Digital Mobility Controllers area. |
| 4 | To enter information about the digital mobility controller, select the row and click in the appropriate cell. |

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Instance	Identifies the location of the DMC.	Numeric	Read/Write
Resource	The name of the DMC.	Alphanumeric	Read/Write
Asset ID	Customer defined tracking number	Initially zero	Read/Write
FRU	Indicates if the unit is considered field replaceable by the manufacturer.	True (if checked)	Read/Write

Viewing and updating other system information

Use the following procedure to view or update other system information. The Other Information area in the Additional Information tab displays other information associated with the selected BCM450 system, such as the name of the administrator and his or her contact information, and the location of the BCM450 system. You can add or update this information. The date on which this information is updated is displayed BCM450 area, in accordance with "LastChangeTime" of the Entity MIB.

Procedure steps

Step	Action
1	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens.
2	Select the Additional Information tab.
3	View the information displayed in the Other Information area at the bottom of the screen.
4	If you want to add or update information about the owner or administrator of the BCM450 system, enter information in the Owner Name field.
5	If you want to add or update other information about the BCM450 system, enter it in the Additional Notes field.

--End--

Variable definitions

Field Name	Field Description	Field Value	Read/Write
Owner name	The owner's name or any other information, such as the administrator's name and contact information	Up to 256 characters	Write
Additional Notes	Additional information about this system.	Up to 256 characters Write	Write
Last change for the system	Date and time when the information was last modified	example '2004-04-16 09:12:00'	Read

Viewing information about devices

The Devices tab displays information about all devices attached to the BCM450. These devices may include:

- digital sets
- analog devices
- IP sets, including IP clients

You can view all Directory Numbers (DNs) and the type of set associated with the DN

Viewing information about attached devices

Use the following procedure to view information about devices attached to the system.

Procedure steps

Step	Action
1	In the BCM450 Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory .
3	The Hardware Inventory panel opens.
4	Click the Devices tab.
5	View the information displayed in the Attached Devices table.
--End--	

Variable definitions

Field Name	Field Description	Field Value	Read/Write
DN	Directory Number	In accordance with DN numbering system	Read
Model	Type of device or set	example T7316 or I2004	Read

Viewing additional information

Use the Additional Information tab to display additional information about the BCM450 main unit, such as:

- details about the manufacturer and the manufacture date
- hardware version details
- serial number details

You require this information only when a field issue requires the identification of certain systems. Items marked on the Element Manager as read-only are detected by the BCM450. For items that are not auto-detected, the Element Manager provides checkboxes, pull-down menus, and fields that the administrator can populate to indicate that these resources are present.

Viewing additional information

Use the following steps to view additional information about the hardware inventory.

Procedure steps

Step	Action
1	In the BCM450 Element Manager, connect to a BCM450 device.
2	Select Administration, General, Hardware Inventory . The Hardware Inventory panel opens.
3	Click the Additional Information tab.
4	View the information displayed in the Additional Information table.
--End--	

Variable definitions

Field Name	Read/Write
Manufacturer*	Read
Manufacture date	Read
BFT/BMB	
BFT FRU PEC code	Read
BFT FRU CPC code	Read
BFT field replaceable	Read
BMB type	Read
BMB serial number	Read
BMB PCP PEC code	Read
BMB PCP CPC code	Read
BMB hardware version	Read
Power Supply	
Resource	Read
Field replaceable	Read
Main Chassis Fans	
Instance	Read
FRU	Read

Attention: Fields marked with an asterisk (*) can also be remotely queried by SNMP using the Entity MIB.

BCM450 software updates

This section describes how to manage BCM450 software updates.

BCM450 software updates navigation

- [Viewing the software update history \(page 145\)](#)
- [Obtaining BCM450 software update \(page 146\)](#)
- [Checking the status of a software update \(page 147\)](#)
- [Applying a software update \(page 147\)](#)
- [Scheduling a software update \(page 155\)](#)
- [Modifying a scheduled software update \(page 158\)](#)
- [Deleting a scheduled software update \(page 159\)](#)
- [Viewing the software inventory \(page 160\)](#)
- [Removing a software update \(page 160\)](#)

Viewing the software update history

Use the following procedure to view the history of updates that have been applied to the BCM450.

Using the Software Update History panel, you can view the history of all software updates, including software upgrades, that have been applied to the BCM450 since the it was shipped. You can:

- view the current software release level of the BCM450
- view a history of all software updates (including upgrades) applied to the BCM450
- view release notes that apply to a particular software update

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.

- 2 Open the **Software Management** folder, and then click the **Software Update History** task.
The Software Update History panel opens
- 3 View the updates in the **Software Update History** table. If software updates have not been applied to your BCM450, the table is empty.
- 4 To view release notes about a particular software update, select the update in the table.
Release notes containing details about the software update are displayed in the Release Notes panel below the table.

--End--

Variable definitions

Columns	Description
Date	The date and time that the software update was applied.
Category	The software update category (Scheduled, Removed, Modified, Applied).
Name	The name of the software update.
Version	The version of the software update.
Description	A brief description of the software update.
Removable	Indicates whether the software update can be removed from the BCM450. If it can be removed, the check box is checked.

Obtaining BCM450 software update

Use the following procedure to obtain a software update. Before you can apply a software update to your BCM450, you must obtain the software update and unzip the file. Authorized Nortel partners can download BCM450 software updates from the Nortel Technical Support web page.

Procedure steps

Step	Action
1	In your web browser, enter www.nortel.com/support and then click the Go button. The Nortel Technical Support Web page opens.
2	Download the required updates.

- 3 Create a directory for each update and unzip the downloaded file into a directory.

--End--

Checking the status of a software update

Use this procedure to view the status of software updates that are transferring or waiting to be transferred, or that are waiting to be applied.

Procedure steps

Step	Action
1	In the task navigation panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens and displays the Updates in Progress tab.
3	View the details in the Updates in Progress table. Once a software update is complete, the entry is removed from the Updates in Progress table and a new entry is added to the Software Update History table to document the installation of the software update.

--End--

Applying a software update

Use the information in this section to apply a software update.

Once you have downloaded a software update from the Nortel Technical Support Web page, you can apply it to the BCM450. You can apply one software update at a time. For multiple software updates, repeat the following procedure until each update has been applied. When you have several updates to apply, any software updates that require the system to reboot should be applied last. Information about each update is available when you click the Show Details button.

This section contains information on the following topics:

- [Applying a software update from your personal computer \(page 148\)](#)
- [Applying a software update from a USB storage device \(page 149\)](#)
- [Applying a software update from a network folder \(page 151\)](#)
- [Applying a software update from an FTP server \(page 152\)](#)
- [Applying a software update from an HTTP server \(page 154\)](#)

Applying a software update from your personal computer

Use the following steps to apply an update from your personal computer.



CAUTION

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



CAUTION

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Procedure steps

Step	Action
1	In the task navigation panel, click the Configuration tab.
2	Select System, Date and Time and verify that the date, time, and time zone are correctly set.
3	In the task navigation panel, click the Administration tab.
4	Open the Software Management folder, and then click the Software Updates task. The Software Update panel opens. The Updates in Progress tab is open.
5	Click the Get New Updates button. The Get New Updates window opens.
6	Select My Computer from the Retrieve From selection field.
7	Click the Browse button. The Select window opens.
8	Navigate to the directory where you unzipped the update file and click Select .

Attention: The Select dialog displays directories only and does not show the contents of the directories.

- 9 Select the location from which you want to retrieve the update.
- The Find Software Updates window opens and displays a list of updates found in the specified location.

Attention: If the information in the **Find Software Updates** window indicates that you are applying an upgrade rather than an update, you will need to generate a keycode before proceeding.

- 10 Select an update. The update must have a status of "Available."
- 11 To view details about the update, click the **Show Details** button.
- The Details for Update window opens and displays any details about the update.
- 12 Click the **OK** button to close the details window.
- 13 Click the **Apply** button to apply the update. A warning dialog box opens.
- 14 Click the **OK** button.
- The Software Update Complete confirmation window opens.
- 15 A dialog box opens to display the options available for this update. The options available depend on the update that you are applying. Select the appropriate options and click the **OK** button. If no options are available, click the **OK** button to continue.
- 16 The **Updates in Progress** table lists the update as **In Progress**. Click the **OK** button.
- A software update that has the Reboot Required field checked automatically restarts the BCM450 once the update has been applied.

--End--

Applying a software update from a USB storage device

Use this procedure to apply an update from a USB storage device.

Prerequisites

Before you apply an update from a USB storage device, make sure that:

- the USB storage device is formatted as a FAT32 device
- you know the path to the location of the updates on the device
- the device is connected to the BCM450
- the size of the software update is not greater than the capacity of the storage device

**CAUTION**

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.

**CAUTION**

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

**CAUTION**

Do not remove the USB storage device until the update is applied. Removing the device before the update has been applied may seriously harm the integrity of your system.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Get New Updates button. The Get New Updates window opens.
4	Select USB Storage Device from the Retrieve From selection field.
5	Enter the path to the location of the update in the Directory field. You must enter the complete path. Click the OK button. The Find Software Updates window opens and displays a list of updates found in the specified location.
6	Select an update. The update must have a status of "Available".

- 7 Click the **Apply** button.
A confirmation window opens.
- 8 Click the **Yes** button.
The Software Update Complete confirmation window opens.
- 9 Click the **OK** button.
The Updates in Progress table lists the update as "In Progress". A software update that has the Reboot Required field checked will automatically reboot the BCM450 once the update has been applied.

--End--

Applying a software update from a network folder

Use this procedure to apply an update from a network folder.



CAUTION

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



CAUTION

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Get New Updates button. The Get New Updates window opens.
4	Select Network Folder from the Retrieve From selection field.
5	Configure the network folder attributes. Click the OK button. T he Find Software Updates window opens and displays a list of updates found in the specified location.
6	Select an update. The update must have a status of "Available"

- 7 Click the **Apply** button.
A confirmation window opens.
- 8 Click the **Yes** button. The **Software Update Complete** confirmation window opens.
- 9 Click the **OK** button.

The Updates in Progress table lists the update as “In Progress”. A software update that has the Reboot Required field checked will automatically reboot the BCM450 once the update has been applied.

--End--

Variable definitions

Attribute	Action
Network Folder	Enter the IP address or host name of the network folder and the resource name. For example, enter \\<hostname>\<resource>.
User Name	Enter the user name associated with the shared folder.
Password	Enter the password of the user.
Directory	Enter the path to the subdirectory of the network folder (optional).

Applying a software update from an FTP server

Use this procedure to apply an update from an FTP server.



CAUTION

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



CAUTION

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Get New Updates button. The Get New Updates window opens.
4	Select FTP Server from the Retrieve From selection field.
5	Configure the FTP Server attributes.
6	Click the OK button. The Find Software Updates window opens and displays a list of updates found in the specified location.
7	Select an update. The update must have a status of "Available".
8	Click the Apply button. A confirmation window opens.
9	Click the Yes button. The Software Update Complete confirmation window opens.
10	Click the OK button. The Updates in Progress table lists the update as "In Progress". A software update that has the Reboot Required field checked will automatically reboot the BCM450 once the update has been applied.

--End--

Variable definitions

Attribute	Description
FTP Server	Enter the IP address or host name of the remote computer, and the port number if required.
User Name	Enter the user name associated with the FTP server.
Password	Enter the user name associated with the FTP server.
Directory	Enter the path to the location of the update. The path is relative to the root of the FTP server you are logging into. For example, if the root of the FTP server you have logged into is /public and your patches are located under /public/patches, you would enter patches as the directory.

Applying a software update from an HTTP server

Use this procedure to apply an update from an HTTP server.



CAUTION

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.



CAUTION

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Attention: The BCM450 supports only Apache web servers as HTTP servers. You must enable automatic index generation on the HTTP server for the directory where the update is located.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Get New Updates button. The Get New Updates window opens.

- 4 Select HTTP Server from the **Retrieve From** selection field.
- 5 Configure the **HTTP Server** attributes.
- 6 Click the **OK** button.
The Find Software Updates window opens and displays a list of updates found in the specified location.
- 7 Select an update. The update must have a status of "Available".
- 8 Click the **Apply** button.
A confirmation window opens.
- 9 Click the **Yes** button.
The Software Update Complete confirmation window opens.
- 10 Click the **OK** button.
The Updates in Progress table lists the update as In Progress. A software update that has the Reboot Required field checked will automatically reboot the BCM450 once the update has been applied.

--End--

Variable definitions

Attribute	Action
HTTP Server	Enter the IP address or host name of the remote computer, and the port number if required.
Use HTTPS	Check this box if the HTTP server requires SSL.
User Name	Enter the user name associated with the HTTP server.
Password	Enter the password of the user.
Directory	Enter the path to the location of the update. The path is relative to the root of the HTTP server you are logging into. For example, if the root of the HTTP server you have logged into is /public and your patches are located under /public/patches, you enter patches as the directory.

Scheduling a software update

You can apply a software update to the BCM450 at a future date by creating a schedule. A scheduled software update is displayed in the Scheduled Updates tab. You can schedule only one update at a time.

You can view, modify, or delete a scheduled software update. When you schedule a software update, the device where the update is stored (such as a USB device) must be connected to the BCM450 when you create the schedule.

**CAUTION**

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.

**CAUTION**

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Procedure steps

Step	Action
1	In the task navigation panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Updates task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Scheduled Updates tab. The Scheduled Software Updates panel opens.
4	Click the Add button. The Get New Updates window opens.
5	In the Retrieve From selection field, select the location where the software update is stored: <ul style="list-style-type: none">• USB Storage Device• My Computer• Network Folder• FTP Server• HTTP Server
6	Select an update location and/or complete the appropriate access information.

- 7 Click the **OK** button.
The New Updates Found window opens and displays a list of updates found in the specified location.
- 8 Select an update. The update must have a status of "Available".
- 9 To view the details for an update, click the **Show Details** button.
The Details for Update window opens and displays any details about the update. Click the OK button to close the details window.
- 10 Click the **Schedule** button to create a schedule.
The Schedule Software Updates window opens.
- 11 Click the **Retrieve** field to select a date and time at which to retrieve the update.
A calendar window opens.
- 12 Select a retrieve date and time, and then close the window.
- 13 Click the **Apply** field to select a date and time at which to apply the update.
A calendar window opens.
- 14 Select a date and time, and then close the window.
- 15 Click the **OK** button.
The software update is added to the Scheduled Software Updates table. The status of the update is "Schedule".

--End--

Variable definitions

Columns	Description
Name	The name of the update.
Version	The version of the update.
Description	A brief description of the update.
Size	The size of the software update, in kilobytes.
Reboot Req'd	Displays whether the software update causes the BCM450 to reboot when the update has been applied. If a reboot is required, the check box is checked.
Location	The storage location of the update. For example, FTP server.
Status	The status of the update. Scheduled—The software update has been scheduled. Removed—The scheduled software update has been deleted. Modified—The scheduled software update has been modified. Applied—The scheduled software update has been applied to the BCM450.
Retrieve	The date and time at which the update will be retrieved.
Apply	The date and time at which the update will be applied.

Modifying a scheduled software update

Use this procedure to modify a scheduled software update.

**CAUTION**

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.

**CAUTION**

If a software update has a checkmark applied against it in the Reboot Req'd column of the Find Software Updates window, the BCM450 will automatically reboot as soon as the update has been applied. You will not receive a reboot confirmation before the reboot occurs.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Scheduled Updates tab.
4	In the Scheduled Software Updates table, select a scheduled update.
5	Click the Modify button. The Modify Scheduled Software Update window opens.
6	Click the Retrieve field to select a date and time at which to retrieve the update. A calendar window opens.
7	Select a retrieve date and time, and then close the window.
8	Click the Apply field to select a date and time at which to apply the update. A calendar window opens.
9	Select an apply date and time, and then close the window.
10	Click the OK button. The modified software update is displayed in the Scheduled Software Updates table. The modification may take a few minutes to appear in the table.

--End--

Deleting a scheduled software update

Use this procedure to delete a scheduled software update.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update task. The Software Update panel opens. The Updates in Progress tab is open.
3	Click the Scheduled Updates tab.

- 4 In the **Scheduled Software Updates** table, select a scheduled update.
- 5 Click the **Delete** button.
The Confirm Delete window opens.
- 6 Click the **Yes** button to delete the update.
The scheduled update is removed from the Scheduled Software Update table.

--End--

Viewing the software inventory

Use this procedure to view the software Inventory.

BCM450 software is organized into software components that you can individually update as required. The version of each software component is tracked so that you can determine the exact software release level of a BCM450 to the component level. The software inventory is a complete list of software components, their version, and the functional group to which they belong.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Inventory task. The Software Inventory panel opens.
3	View the details in the Software Component Version Information table. You can change the order of the information displayed in the table by clicking a column heading and dragging it to a new place in the table. You can also sort the information in a column by descending or ascending order, by clicking the column heading.

--End--

Removing a software update

Use this procedure to remove a software update that has been applied to the BCM450. Not all software updates can be removed; whether a software update can be removed depends on the particular software update. Removing

a software update does not remove the software itself from the BCM450; it only returns the software components of the software update to a previous software version.

You must have administrator privileges to remove a software update from the BCM450. Removing a software patch or upgrade from the BCM450 is a service-affecting operation. All services running on the system will be stopped. Consequently, Nortel recommends that you schedule removal of updates for low-traffic periods. If a software update is applied to a BCM450 and then removed, this information is displayed in the Software Update History table. A removal operation is logged by the BCM450, but does not generate an alarm condition. You can remove a software update if the update has a checkmark in the Removable column of the Software Update History table.

**CAUTION**

Applying a software update to the BCM450 is a service-affecting operation. Nortel recommends that you schedule updates for low-traffic hours.

Procedure steps

Step	Action
1	In the task panel, click the Administration tab.
2	Open the Software Management folder, and then click the Software Update History task. The Software Update History panel opens.
3	Select an update in the Software Update History table. The update must have a checkmark against it in the Removable column.
4	Click the Remove Software Update button. A confirmation window opens.
5	Click Yes . The Category column in the Software Update History table displays "Patch Removed" for the removed software update.

--End--

BCM450 utilities

This section contains information about how to use BCM450 utilities within Element Manager to assist in performing administrative tasks for your BCM450 system.

BCM450 utilities navigation

- [Pinging a device \(page 163\)](#)
- [Tracing a route \(page 164\)](#)
- [Viewing Ethernet activity \(page 164\)](#)
- [Resetting and rebooting \(page 165\)](#)
- [Creating a scheduled reboot \(page 167\)](#)
- [Modifying a scheduled reboot \(page 168\)](#)
- [Deleting a scheduled reboot \(page 169\)](#)
- [Setting release reasons \(page 169\)](#)
- [Command Line Interface \(page 170\)](#)

Pinging a device

Use this procedure to ping a device. You can ping a device to verify that a route exists between the BCM450 and another device.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder click Ping . The Ping panel opens.
3	In the Address box, enter the IP address of the element you want to ping.
4	Click Ping . The results appear in the Results area.

--End--

Tracing a route

Use this procedure to start a trace to measure round-trip times to all hops along a route. This helps you to identify bottlenecks in the network.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Trace Route . The Trace Route panel opens.
3	In the Maximum number of hops box, enter the maximum number of hops on the route.
4	In the Address box, enter the IP address of the element for which you want to perform a trace route.
5	Click Trace Route . The results are displayed in the Results area.

--End--

Viewing Ethernet activity

Use this procedure to view Ethernet activity in the BCM450 system.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Ethernet Activity . The Ethernet Activity panel opens.
3	In the Ethernet Activity area, click Retrieve . Details are displayed in the Results area.

--End--

Resetting and rebooting

Use the Reset utility to perform a warm-reset, cold-reset, or reboot of your BCM450 system.

Warm reset

Use this procedure to restart all telephony services, including LAN CTE, voice mail, and IP telephony. This operation does not affect configuration parameters or programming.



CAUTION

All active calls on the BCM450 system will be dropped.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reset . The Reset panel opens.
3	Click Warm Reset Telephony Services . A confirmation dialog box appears.
4	Click OK . All telephony services are restarted, including LAN CTE, voice mail, and IP telephony.

--End--

Cold reset

Use this procedure to perform a cold reset. A cold reset of the BCM450 resets telephony programming of the BCM450 system to the factory defaults for that software level.



CAUTION

Performing a cold reset of telephony services erases all telephony programming, as well as all Voice Message mailboxes and messages. Telephony services will restart with all telephony programming at default values for the specified region, template, and start DN, for the current software release level.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reset . The Reset panel opens.
3	Click Cold Reset Telephony Services . The Cold Reset Telephony dialog box appears.
4	Configure the Cold Reset Telephony attributes.
5	Click OK . All telephony services are reset, including LAN CTE, voice mail, and IP telephony.

--End--

Variable definitions

Variable	Value
Region	Specify the startup region.
Template	Specify the startup template. Options are: PBX or DID.
Start DN	Specify the startup DN. The default value is 221.

Rebooting

Use this procedure to reboot the system. Rebooting the BCM450 system temporarily stops all services running on the system and then restarts all services.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reset . The Reset panel opens.
3	Click Reboot System . A confirmation dialog box appears.

-
- 4 Click **OK**.
The operating system of the BCM450 restarts.
-

--End--

Creating a scheduled reboot

Use this procedure to create a scheduled reboot. This procedure allows you to specify a one-time or reoccurring reboot schedule.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reboot . The Reboot panel opens.
3	Select the Scheduled Reboot tab. The Scheduled Reboot screen appears.
4	Click Add . The Add Scheduled Reboot Screen appears.
5	Enter a memo for the schedule in the Memo field.
6	Select Once, Daily, Weekly, or Monthly from the Recurrence field.
7	Select the month you want the reboot to occur.
8	Enter the day of the month you want the reboot to occur.
9	Enter the time you want the reboot to occur.
10	Click Ok .

--End--

Variable definitions

Variable	Value
Memo	Allows you to add a title or a note to the scheduled reboot. This is displayed in the Memo field of the Scheduled Reboot table.
Recurrence	Specify how often you want the reboot to occur. Options are: Once, Daily, Weekly, or Monthly.
Month	Specify the month you want the reboot to occur.
Day of month	Specify the day of month you want the reboot to occur.
Time	Specify the time you want the reboot to occur.

Modifying a scheduled reboot

Use this procedure to modify an existing scheduled reboot.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reboot . The Reboot panel opens.
3	Select the Scheduled Reboot tab. The Scheduled Reboot screen appears.
4	Select the Scheduled Reboot you want to modify.
5	Click Modify . The Modify Scheduled Reboot Screen appears.
6	Enter a memo for the schedule in the Memo field.
7	Select Once, Daily, Weekly, or Monthly from the Recurrence field.
8	Select the month you want the reboot to occur.
9	Enter the day of the month you want the reboot to occur.
10	Enter the time you want the reboot to occur.
11	Click Ok .

--End--

Variable definitions

Variable	Value
Memo	Allows you to add a title or a note to the scheduled reboot. This is displayed in the Memo field of the Scheduled Reboot table.
Recurrence	Specify how often you want the reboot to occur. Options are: Once, Daily, Weekly, or Monthly.
Month	Specify the month you want the reboot to occur.
Day of month	Specify the day of month you want the reboot to occur.
Time	Specify the time you want the reboot to occur.

Deleting a scheduled reboot

Use this procedure to delete an existing scheduled reboot.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click Reboot . The Reboot panel opens.
3	Select the Scheduled Reboot tab. The Scheduled Reboot screen appears.
4	Select the Scheduled Reboot you want to delete.
5	Click Delete . The confirmation window appears.
6	Click Yes to delete the scheduled reboot.
--End--	

Setting release reasons

Use this procedure to determine the level of system reporting you require for released ISDN or VoIP calls.

Procedure steps

Step	Action
1	Click the Administration tab.

- 2 From the **Utilities** folder, click **Diagnostic settings**.
The Diagnostic settings panel opens.
- 3 Click the **Telephony** tab.
The Release Reasons panel opens.
- 4 From the **Release Reasons** list select the level of reporting that you require.

--End--

Variable definitions

Variable	Value
None	No text will accompany a dropped call notification.
Simple	A simple explanation of the Cause code is provided. Select the Cause Code check box to provide only the cause code with a dropped call notification. Clear the Cause Code check box to provide text and the cause code with a dropped call notification.
Detailed	A detailed explanation of the Cause code is provided.

Command Line Interface

You can use the Command Line Interface (CLI) to configure basic settings, as well as shut down, reboot, or perform a Level 1 or Level 2 reset the BCM450 system. Two CLI modes are available: Maintenance CLI, and Configuration CLI.

Your user account must be assigned the System-CLI privilege in order to access the CLI. For information about how to access the CLI, refer to the BCM450 Troubleshooting Guide (NN40160-700).

This section contains information about the following topics:

- [Configuration CLI \(page 170\)](#)
- [Maintenance CLI \(page 171\)](#)

Configuration CLI

The Configuration CLI displays when the system is in Main OS mode. The options available on the Configuration CLI are:

- 0—Exit. The system exits the CLI to the login prompt.
- 1—Reboot. The system reboots to the Main OS.
- 2—Shutdown. The system shuts down. You need physical access to the BCM450 hardware to restart the system.

- 3—Safe OS. The system reboots to the Safe OS and waits 1 minute for you to login. When you login within 1 minute, the Maintenance CLI displays. If you do not login within 1 minute, the system changes to the Main OS.
- 4—Configuration Reset. A Level 1 reset occurs. The system resets all configuration data to the factory defaults.
- 5—Software Reset. A Level 2 reset occurs. The system resets all configuration data and software to the factory defaults.
- 6—IP Configuration. You can configure the following basic IP settings:
 - 0—Return to Previous Menu. The system returns to the main menu.
 - 1—Hostname. Provision the hostname of the system.
 - 2—IP Address. Provision the IP address of the system.
 - 3—Subnet Mask. Provision the subnet mask for the IP address.
 - 4—Default Gateway. Provision the default gateway for the system.
 - 5—DHCP Client Mode. Enable or disable the DHCP client.
 - 6—Commit Changes. Save changes to the IP settings.
 - 7—Reload Settings. Reload the existing IP settings.

Maintenance CLI

The Maintenance CLI displays when the system is in Safe OS mode. The Safe OS is a diagnostic mode that you can use if the Main OS is experiencing problems. No applications or telephony services are running when the BCM450 is in Safe OS mode. The options available on the Maintenance CLI are:

- 0—Exit. The system exits to the Safe OS login prompt.
- 1—Reboot into Main OS. The system reboots to the Main OS.
- 2—Shutdown. The system shuts down. You need physical access to the BCM450 hardware to restart the system.
- 3—Reboot into Safe OS. The system reboots to the Safe OS and waits 1 minute for you to login. If you do not login within 1 minute, the system changes to the Main OS.
- 4—Transition to Main OS. The system changes from the Safe OS to the Main OS without restarting.
- 5—Configuration Reset. A Level 1 reset occurs. The system resets all configuration data to the factory defaults.
- 6—Software Reset. A Level 2 reset occurs. The system resets all configuration data and software to the factory defaults.

BCM Monitor installation and removal

BCM Monitor is included with the installation of Element Manager. You do not need to download and install the utility separately, unless you are an administrative user who requires access to only this management tool, and you do not have or require Element Manager.

BCM Monitor installation and removal navigation

- [Installing BCM Monitor \(outside Element Manager\) \(page 173\)](#)
- [Removing BCM Monitor \(outside Element Manager\) \(page 174\)](#)

Installing BCM Monitor (outside Element Manager)

You can download and install BCM Monitor separately from Element Manager if you are an administrative user who requires access to only this management tool, and you do not have or require Element Manager.

Prerequisites

- Connect to your BCM450 system and access the BCM450 Web page.
- For security reasons, the user on the computer on which the BCM Monitor runs must be authenticated by the BCM450 system.

Procedure steps

Step	Action
1	In your web browser, type the IP address of the BCM450 and click the Go button. The login screen displays.
2	Log in using the same username and password that you use to access the Element Manager. The BCM450 Web Page opens.
3	Click the Administrator Applications link. The Administrator Applications page appears.

- 4 Click the **BCM Monitor** link.
The BCM Monitor page appears.
- 5 Click the **Download BCM Monitor** link.
- 6 Click **Save** or click **Run** to run the install file directly from the Web page.
- 7 If you clicked **Save**, the **Download complete** dialog box notifies you when the download has finished. Go to the folder where you saved the BCM Monitor install file, and then double-click the BCMMonitor.exe icon.
- 8 Follow the instructions on the installation wizard.

--End--

Removing BCM Monitor (outside Element Manager)

If you do not require BCM Monitor on your computer, you can remove it from your computer.

Procedure steps

Step	Action
1	In Windows, click Start .
2	Select Settings > Control Panel .
3	Double-click Add or Remove Programs .
4	Select BCM Monitor , and then click Change/Remove .
5	Follow the on-screen removal instructions.

--End--

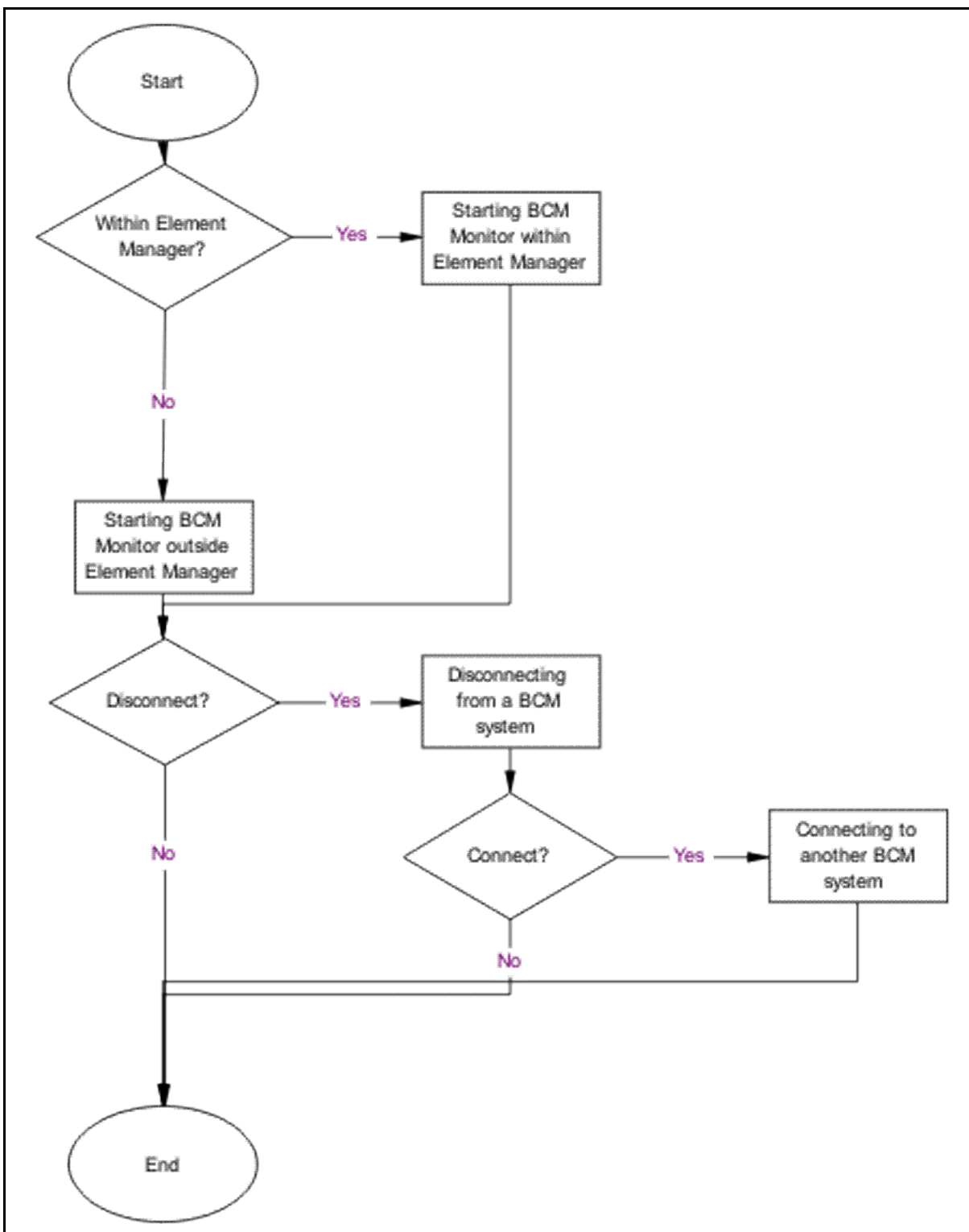
BCM Monitor connection

You can start BCM Monitor from within Element Manager or outside of Element Manager. You can also disconnect BCM Monitor from the current system and connect to another system.

BCM Monitor connection procedures

This task flow shows you the sequence of procedures you perform to start BCM Monitor. To link to any procedure, click on [BCM Monitor connection navigation](#).

Figure 4 BCM Monitor connection procedures



BCM Monitor connection navigation

- [Starting BCM Monitor within Element Manager \(page 177\)](#)
- [Starting BCM Monitor outside Element Manager \(page 177\)](#)
- [Disconnecting from a BCM system \(page 178\)](#)
- [Connecting to another BCM system \(page 178\)](#)

Starting BCM Monitor within Element Manager

You can launch BCM Monitor from within Element Manager.

Prerequisites

- Launch Element Manager and connect to your BCM450 system.

Procedure steps

Step	Action
1	Click the Administration tab.
2	From the Utilities folder, click BCM Monitor . The BCM Monitor pane appears.
3	Click Launch BCM Monitor . BCM Monitor appears and connects to the same BCM450 that the Element Manager is currently connected to.
--End--	

Starting BCM Monitor outside Element Manager

Start BCM Monitor without launching Element Manager or if you do not have Element Manager installed on your computer.

Procedure steps

Step	Action
1	Double-click the BCM Monitor shortcut on your desktop or select BCM Monitor in your Start/Programs menu. The Enter Logon Information window appears.
2	In the System Name or IP Address box, enter the system name of the BCM450 you want to monitor.
3	In the Connect As box, enter your BCM450 user name.

- 4 In the **Password** box, enter the password associated with your BCM450 user name.
- 5 Click **Connect**.
The BCM Monitor pane appears.

--End--

Disconnecting from a BCM system

Disconnect BCM Monitor from your BCM450 system.

Prerequisites

- Start BCM Monitor. For more information, see [Starting BCM Monitor within Element Manager \(page 177\)](#) or [Starting BCM Monitor outside Element Manager \(page 177\)](#).

Procedure steps

Step	Action
1	On the File menu, choose Disconnect from BCM . BCM Monitor disconnects from the BCM450 system and clears all the fields.
2	If you do not want to connect to another BCM450 system, close the BCM Monitor application. This terminates the application and disconnects BCM Monitor from the BCM450 system.

--End--

Connecting to another BCM system

Connect BCM Monitor to another BCM450 system.

Prerequisites

- Disconnect BCM Monitor from your current BCM450 system. For more information, see [Disconnecting from a BCM system \(page 178\)](#).

Procedure steps

Step	Action
1	On the File menu, choose Connect to BCM . The Enter Logon Information window appears.

- 2 In the **System Name or IP Address** box, enter the system name of the BCM450 you want to monitor.
- 3 In the **Connect As** box, enter your BCM450 user name.
- 4 In the **Password** box, enter your password.
- 5 Click **Connect**.
The BCM Monitor pane appears.

--End--

Using BCM Monitor

This section describes how to use BCM Monitor to capture and review data about the BCM450 system.

Using the BCM Monitor navigation

- [System status snapshots \(page 181\)](#)
- [UIP information analysis \(page 186\)](#)
- [Line summary \(page 191\)](#)
- [BCM Monitor statistics \(page 191\)](#)

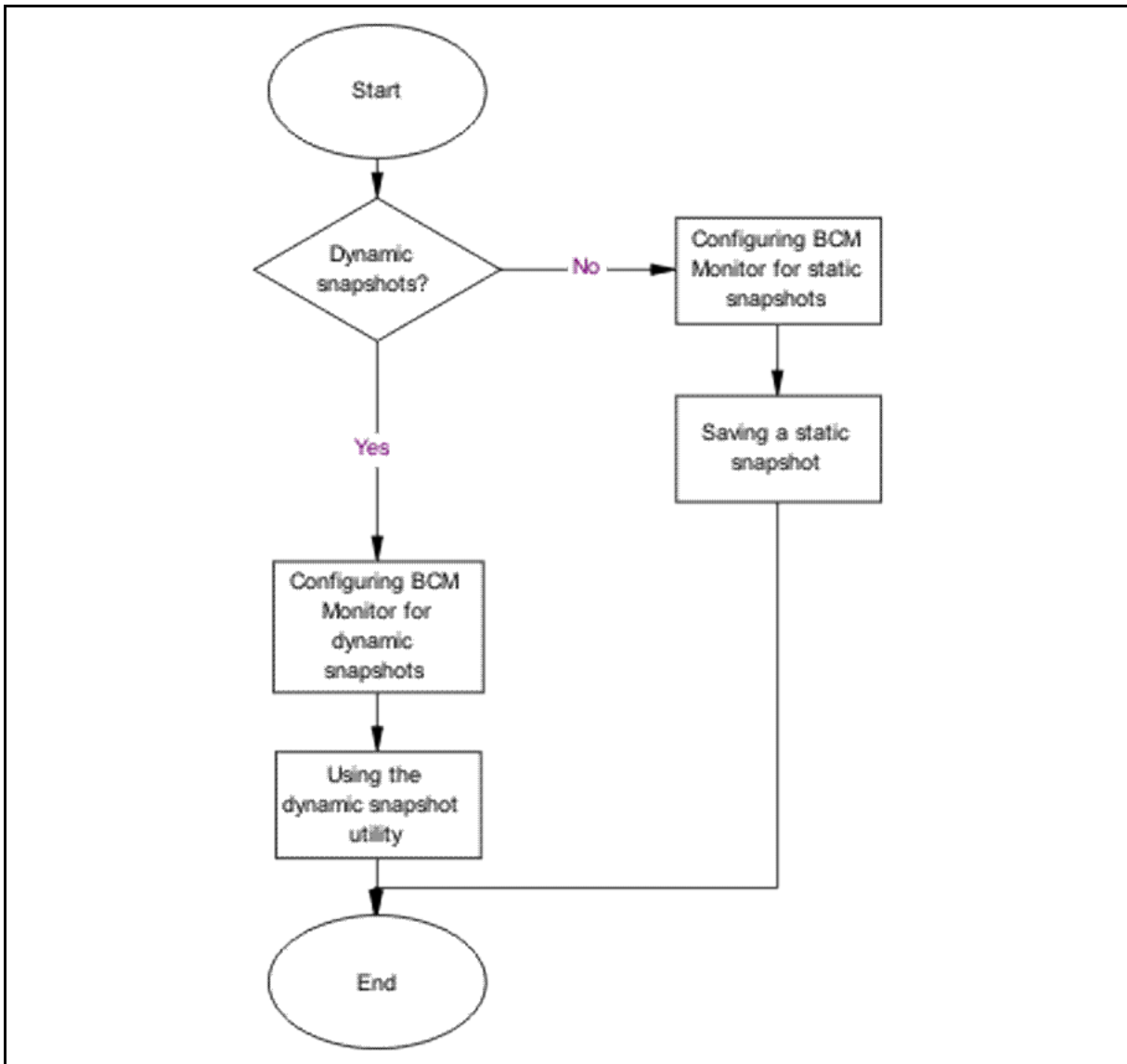
System status snapshots

You can capture static and dynamic snapshots of system information in a text file. For static snapshots, you specify which BCM Monitor tab you want to capture. Dynamic snapshots record snapshots of system data that changes over time, such as CPU utilization and active calls. The system captures dynamic snapshots according to a frequency that you define.

System status snapshot procedures

This task flow shows you the sequence of procedures you perform to work with system status snapshots. To link to any procedure, click on [BCM450 system status snapshots navigation](#)

Figure 5 BCM450 system status snapshots procedures



BCM450 system status snapshots navigation

- [Configuring BCM Monitor for static snapshots \(page 182\)](#)
- [Saving a static snapshot \(page 184\)](#)
- [Configuring BCM Monitor for dynamic snapshots \(page 184\)](#)
- [Using the dynamic snapshot utility \(page 186\)](#)

Configuring BCM Monitor for static snapshots

Configure BCM Monitor with the desired settings for static snapshots.

Procedure steps

Step	Action
1	On the File menu, choose Snapshot Settings . The Snapshot Settings pane appears.
2	Click the Static snapshot settings tab.
3	In the Output Filename box, enter the filename for the static snapshot. For additional options, click the arrow button to the right of the Output Filename box.
4	In the Output Folder box, enter the path of the folder where you want to store static snapshots. To browse for a folder, click ... to the right of the Output Folder box. The Browse for Folder dialog box appears.
5	Select a folder or make a new folder, and then click OK .
6	Select the BCM Monitor tabs that you want to include in static snapshots in the Tabs Saved in Snapshot box. For example, if you want snapshots to include information about voice ports, make sure that Voice Ports is included in the Tabs Saved in Snapshot box.
7	To remove tabs from the snapshots definition, select a tab from the Tabs Saved in Snapshot box and use the arrow button to move the tab to the Tabs Not Saved in Snapshot box.
8	Click OK .

--End--

Variable definitions

Variable	Value
Auto-Increment Counter	Automatically increments the filename so that subsequent files do not overwrite earlier files. Adds <counter> to the filename in the Output Filename box.
BCM Name	Adds the name of the BCM to the filename. Position your cursor in the filename box where you want the name to be added. Adds <BCM name> to the filename in the Output Filename box.
Time	Adds the time to the filename. Position your cursor in the filename box where you want the name to be added. Adds <time> to the filename in the Output Filename box.
Date	Adds the date to the filename. Position your cursor in the filename box where you want the name to be added. Adds <date> to the filename in the Output Filename box.

Saving a static snapshot

After you have configured static snapshot settings, you can save a static snapshot at any time.

Prerequisites

- Configure BCM Monitor for static snapshots. For more information, see [Configuring BCM Monitor for static snapshots \(page 182\)](#).

Procedure steps

Step	Action
1	<p>While you are observing data on a tab, on the File menu, choose Save Static Snapshots or press Ctrl+s.</p> <p>All the tabs included in the snapshot definition are saved to a text file in the folder you specified when you configured the static snapshot settings.</p>

--End--

Configuring BCM Monitor for dynamic snapshots

Dynamic snapshots record snapshots of system data that changes over time, such as CPU utilization and active calls.

Procedure steps

Step	Action
1	On the File menu, select Snapshot Settings . The Snapshot Settings panel opens.
2	Click the Dynamic Snapshot Settings tab.
3	In the Output Filename box, enter the filename for the dynamic snapshot. For additional options, click the arrow button to the right of the Output Filename box.
4	Configure the Output Filename attributes.
5	In Output Folder box, enter the path of the folder where you want to store the static snapshots. To browse for a folder, click the ... button to the right of the Output Folder box. The Browse for Folder dialog box appears.
6	Select a folder or make a new folder, and then click OK .
7	Select the BCM Monitor tabs that you want to include in dynamic snapshots in the Tabs Saved in Snapshot box. For example, if you want the snapshots to include information about voice ports, make sure that Voice Ports is included in the Tabs Saved in Snapshot box.
8	To remove a tab from the snapshots, select a tab from the Tabs Saved in Snapshot box and use the arrow button to move the tab to the Tabs Not Saved in Snapshot box.
9	In the Automatic Snapshot area, click the Enable Automatic Snapshot check box to enable automatic snapshots. If you disable automatic snapshots, BCM Monitor will take a single snapshot instead of a series of snapshots. If you enable automatic snapshots, the Automatic Snapshot Interval (sec) box and the Number of Snapshots box become available.
10	In the Automatic Snapshot Interval (sec) box, enter the interval in seconds between successive automatic snapshots.
11	In the Number of Snapshots box, enter the number of snapshots from 1 to Infinite.
12	Click OK .

--End--

Variable definitions

Variable	Value
Auto-Increment Counter	Automatically increments the filename so that subsequent files do not overwrite earlier files. Adds <counter> to the filename in the Output Filename box.
BCM Name	Adds the name of the BCM to the filename. Position your cursor in the filename box where you want the name to be added. Adds <BCM name> to the filename in the Output Filename box.
Time	Adds the time to the filename. Position your cursor in the filename box where you want the name to be added. Adds <time> to the filename in the Output Filename box.
Date	Adds the date to the filename. Position your cursor in the filename box where you want the name to be added. Adds <date> to the filename in the Output Filename box.

Using the dynamic snapshot utility

After you have configured dynamic snapshot settings, you can start and stop the dynamic snapshot utility.

Prerequisites

- Configure BCM Monitor for dynamic snapshots. For more information, see [Configuring BCM Monitor for dynamic snapshots \(page 184\)](#).

Procedure steps

Step	Action
1	To start the dynamic snapshot utility, on the File menu, select Dynamic Snapshot > Start . BCM Monitor starts taking snapshots and saves the snapshot data in a file located in the folder you specified when you configured the dynamic snapshot settings.
2	To stop the dynamic snapshot utility, on the File menu, select Dynamic Snapshot > Stop .

--End--

UIP information analysis

The Universal ISDN Protocol (UIP) tab allows you to enable monitoring of UIP messages associated with IP trunks (MCDN messages) and PRI modules installed in the monitored BCM system.

This section contains the following topics:

- [Enabling UIP message monitoring \(page 187\)](#)
- [Disabling UIP message monitoring \(page 188\)](#)
- [Logging UIP data \(page 189\)](#)
- [Accessing UIP log files \(page 189\)](#)
- [Disabling UIP timeout settings \(page 189\)](#)
- [Accessing message detail information elements \(page 190\)](#)
- [Clearing message detail information elements \(page 190\)](#)

Enabling UIP message monitoring

Enable monitoring of UIP messages associated with IP trunks (MCDN messages) and PRI modules installed in the monitored BCM450 system.

Prerequisites



CAUTION

Monitoring UIP messages can affect the performance of the BCM450 system or connected peripherals. For example, if IP sets or voice ports make or receive a high number of calls over PRI trunks, monitoring UIP increases the amount of signalling data and can increase the response time for IP sets or voice ports. Therefore, it is strongly recommended that you monitor only a single UIP module at a time and restrict the monitoring time.

Procedure steps

Step	Action
1	Click the UIP tab.
2	Select the MCDN over IP check box.
3	To select an expansion module, select one of the following from the Bus list: <ul style="list-style-type: none">• Bus 3• Bus 5• Bus 7

- 4 Select the type of ISDN modules:
 - PRI — enables monitoring of a DTI module
 - BRI — enables monitoring of BRI loops

--End--

Example of enabling UIP message monitoring

For example, you can monitor UIP messages for loops 1 and 2 of a BRI module connected to Bus 5 and a PRI module connected to Bus 6.

Step	Action
1	Select Bus 5 - BRI.
2	Select Module 1 - Loop 1.
3	Select Module 1 - Loop 2.
4	Select Bus 7 - PRI.

--End--

Disabling UIP message monitoring

Disable monitoring of UIP messages associated with IP trunks (MCDN messages) and PRI modules installed in the monitored BCM450 system.

Procedure steps

Step	Action
1	Click the UIP tab.
2	Clear the MCDN over IP check box.
3	From the Bus list, select the bus you want to disable.
4	Select the Off option button.

--End--

Logging UIP data

You can log UIP data to track the most recent 20 UIP messages.

Procedure steps

Step	Action
1	Click the UIP tab.
2	Select the Log UIP Data check box.
--End--	

Accessing UIP log files

If you enable UIP logging, BCM Monitor writes UIP messages in log files, which are created in the log folder in the BCM Monitor startup directory. One log file is generated for each monitored system and each module or loop.

Procedure steps

Step	Action
1	Locate the log file that is saved to the BCM Monitor startup directory. Log files are named IPAddr_MCDN.log, IPAddr_PRI_BusX.log, and IPAddr_BRI_BusXModuleYLoopZ.log.
2	Open the log file with a text editor, such as Notepad, or a spreadsheet application, such as Microsoft Excel. You can view the amount of time after which monitoring of selected UIP modules will be disabled, and you can disable the monitoring timeout. If you are investigating intermittent problems, an extended monitoring period can be required. In this case, disable the monitoring timeout and enable logging of UIP data.
--End--	

Disabling UIP timeout settings

Disabling UIP timeout settings allows you to override the UIP monitoring timeout.

Prerequisites

- Before you disable the monitoring timeout, consider the potential impact on system performance if the BCM450 system handles a high number of PRI calls.

Procedure steps

Step	Action
1	Click the UIP tab.
2	Select the Disable Timeout check box.

--End--

Accessing message detail information elements

You can view message details to get more information about a UIP message.

Procedure steps

Step	Action
1	Click the UIP tab. The Universal ISDN Protocol Messages area displays detailed information about monitored UIP modules.
2	In the Universal ISDN Protocol Messages area, double-click a UIP message. Information elements appear below the UIP message.

--End--

Clearing message detail information elements

Clear message details after you have viewed the message detail information.

Procedure steps

Step	Action
1	Click the UIP tab. The Universal ISDN Protocol Messages area displays detailed information about monitored UIP modules.
2	In the Universal ISDN Protocol Messages area, right-click a UIP message or information element and then click Clear Tree . The entire tree is cleared from the Universal ISDN Protocol Messages area.

--End--

Line summary

The Line Monitor tab provides real time information about the state of all physical and voice over IP (VoIP) lines on the BCM system.

Procedure steps

Step	Action
1	Click the Line Monitor tab.
2	Select the Show All Lines (Including Inactive) check box. The Line Monitor area displays all lines on the BCM450 system. For lines displayed in light gray, previous calls are shown until a new call is placed or received on that line.
--End--	

BCM Monitor statistics

This section contains information on the following topics:

- [Viewing current, minimum, and maximum values \(page 191\)](#)
- [Resetting logged minimum and maximum values \(page 192\)](#)

Viewing current, minimum, and maximum values

Use BCM Monitor to view the current, minimum, and maximum values of a parameter.

Procedure steps

Step	Action
1	On one of the BCM Monitor panes, click the statistical value for which you want to view the current, minimum, and maximum values. The current (Cur:), minimum (Min:), and maximum (Max:) values appear on the Status bar at the bottom of the panel. The values remain on the Status bar, until another statistical value to view is selected.
2	To view the date and time for the statistical values, on the Statistics menu, select Show Min/Max Times . A dialog box appears with the date and time when the minimum and maximum values occurred.

- 3 Click **OK** to close the dialog box.

--End--

Resetting logged minimum and maximum values

Reset the minimum and maximum values, to delete the current minimum and maximum values and start recording new values.

Procedure steps

Step	Action
1	Click the statistical value you want to reset.
2	To reset only the selected statistical value, on the Statistics menu, select Reset Current Min/Max .
3	To reset the statistical values for all statistics, on the Statistics menu, select Reset All Min/Max .

--End--

BCM450 service management system

This section describes how to view and administer the services that run on the BCM450 system.

You can view details about the services that run on the BCM450 system, including:

- the name of a service
- whether a service is enabled to automatically start up
- the status of the service running on the BCM450

You can also administer services by starting, stopping, and restarting certain services.

Attention: Use the BCM450 Services Manager only as directed by Nortel Technical Support. Improper use of the BCM450 Services Manager may adversely affect system operation.

Service name	Description
ActRptProviderAgent	
BCMClipPasswordFlush	
BCMSetTemplateProviderAgent	
BCMWebProviderAgent	Cimom Provider
BCM_Doorphone	Doorphone Service
BCM_LicenseProviderAgent	Cimom Provider
BCM_NATDialinProviderAgent	
BackupRestoreProviderAgent	Cimom Provider
BriSW	BRI software
CCRSAppServer	
CDRService	Call Detail Recording Service
Core Tel	Core Telephony

Service name	Description
Cte	Computer Telephony Engine
DHCPProviderAgent	Cimom Provider
DiaLogger	System Logging Mechanism
Echo Server	echo service
HGMetrics Reporter	Hunt Group Metrics
IpTelProviderAgent	Cimom Provider
LANProviderAgent	Cimom Provider
Msm	Media Services Manager
MsmProviderAgent	Cimom Provider
NnuScheduler	System Scheduler
OneButton Text	
Pdrd	Persistence Data Repository Service
SoftwareUpdateProviderAgent	Cimom Provider
SyslogListener	Syslog Receiver
UftpServer	UFTP Server
WANFailoverProvider Agent	Cimom Provider
WANSERVICEMgr	WAN Service
apcupsd	
btraceserver	Plug-in for Authentication and Routing Management for BT
core_file_monitor	core file monitoring service
crond	Cron Scheduler
cti server	CTI service
feps	Functional Endpoint Proxy Server (VoIP Gateway)
httpd	HTTP Daemon
lms	Line Monitor Server
mgs	Media Gateway Server
mib2agt	MIB II service
modemcc	modem service
mps	IP Telephony—Media Path
owcimomd	Open Wbem Cimom Server Daemon
psm	—

Service name	Description
qmond	QoS Monitor
securityservice	Authentication and Authorization
srg	SRG service
ssba	System Set Based Admin Service (Feature 9*8)
sshd	Secure Shell Daemon
tmwservice	Time Service
utps	UniSTIM Terminal Proxy Server (IP Sets)
voicemail	Voicemail Process

Managing services

This section contains information on the following topics:

- [Viewing details about services \(page 195\)](#)
- [Stopping a service \(page 195\)](#)
- [Restarting a service \(page 196\)](#)

Attention: Use the BCM450 Services Manager only as directed by Nortel Technical Support. Improper use of the BCM450 Services Manager may adversely affect system operation.

Viewing details about services

Use the following procedure to view details about the services running on the BCM450 system.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the General folder, and then click the Service Manager task. The Service Manager page opens. Services are displayed in the Services table.

--End--

Stopping a service

Use the following procedure to stop any of the services that are running on the BCM450 system.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the General folder, and then click the Service Manager task. The Service Manager page opens. Services are displayed in the Services table.
3	In the Services table, select a service.
4	Click the Stop button.
5	A confirmation dialog box opens.
6	Click Yes . In the Services table, Stopped is displayed in the Status column for the stopped service

--End--

Restarting a service

Use the following procedure to restart any of the services that are running on the BCM450 system.

Procedure steps

Step	Action
1	Click the Administration tab.
2	Open the General folder, and then click the Service Manager task. The Service Manager page opens. Services are displayed in the Services table.
3	In the Services table, select a stopped service.
4	Click the Restart button. A confirmation dialog box opens.
5	Click Yes .
6	In the Services table, Running is displayed in the Status column for the restarted service.

--End--

BCM450 Management Information Bases

This section describes the Management Information Bases (MIBs) supported by the BCM450. A MIB is a virtual information store that contains a collection of objects that are managed using Simple Network Management Protocol (SNMP). The MIB is software that defines the data reported by a computing or network device and the extent of control over that device.

Accessing MIB files

You access MIB files from the BCM504 Web Page. You can also access BCM450 MIB files as a zipped file from the Nortel Customer Service Site.

Accessing MIB files from the BCM450 web page

Use the following procedure to download MIB files from the BCM450 web page.

Procedure steps

Step	Action
1	Go to the BCM450 web page.
2	Click the Administration Applications link.
3	Click BCM MIBs .
4	Click Download Device MIBs . A File Download dialog box displays.
5	Click Save to download the file.

--End--

Accessing MIB files from the Nortel Customer Service site

Use the following procedure to download MIB files from the Nortel Customer Service site.

Procedure steps

Step	Action
1	In your browser, go to http://www.nortel.com . The Nortel Customer Service Site home page opens. If you used the direct link, the Technical Support page opens. Go to step 5.
2	Select the Support & Training navigation menu, and then select Technical Support, Software Downloads . The Technical Support page opens. The Browse Product Support tab displays Product Finder fields.
3	In area 1, select Product Families from the selection field, and then select BCM from the selection box.
4	In area 2, select Business Communications Manager (BCM) .
5	In area 3, select Software .
6	Click the Go link. The Software tab opens.
7	In the by Title/Number Keyword field, enter <code>mib</code> , and then press the Enter key. A list of MIBs is displayed.
8	In the Title column, click the BCM450 MIB link. The Software Detail Information page opens.
9	Right-click the BCM450 MIB link, and select Save Target As . The File Download dialog box opens.
10	In the Save As dialog box, select the file or folder in which you want to save the MIB zip file, and then click the Save button. The MIB zip file is saved to your personal computer.

--End--

Nortel Business Communications Manager 450 1.0

Administration and Security

Copyright © 2008-2009, Nortel Networks. The information in this document is sourced in Canada, the United States, India and the United Kingdom.
All Rights Reserved.

Publication: NN40160-601
Document status: Standard
Document issue: 01.02
Document date: July 2009
Product release: BCM450 1.0
Job function: Administration and Security
Type: Technical Publication
Language type: EN

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.
Windows is a trademark of Microsoft Corporation.
All other trademarks are the property of their respective owners.

To provide feedback or report a problem with this document, go to www.nortel.com/documentfeedback.

